CLOSED, CV, PATENT, PHV

U.S. District Court
U.S.District Court Minnesota (DMN)
CIVIL DOCKET FOR CASE #: 0:07-cv-02198-JMR-FLN

Secure Computing Corporation v. Finjan Software Ltd et al
Assigned to: Chief Judge James M. Rosenbaum
Referred to: Magistrate Judge Franklin L. Noel
Cause: 35:183 Patent Infringement

Date Filed: 05/04/2007
Date Terminated: 08/16/2007
Jury Demand: Plaintiff
Nature of Suit: 830 Patent
Jurisdiction: Federal Question

Plaintiff

Secure Computing Corporation represented by **Christopher A Seidl**
Robins Kaplan Miller & Ciresi LLP
800 LaSalle Ave Ste 2800
Minneapolis, MN 55402-2015
612-349-8468
Email: caseidl@rkmc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jacob M Holdreith
Robins Kaplan Miller & Ciresi LLP
800 LaSalle Ave Ste 2800
Minneapolis, MN 55402-2015
612-349-8500
Fax: 612-339-4181
Email: jmholdreith@rkmc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Ronald J Schutz
Robins Kaplan Miller & Ciresi LLP
800 LaSalle Ave Ste 2800
Minneapolis, MN 55402-2015
612-349-8500
Fax: 612-339-4181
Email: rjschutz@rkmc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Trevor J Foster
Robins Kaplan Miller & Ciresi LLP
800 LaSalle Ave Ste 2800
Minneapolis, MN 55402-2015
612-349-0859
Fax: 612-339-4181
Email: tjfoster@rkmc.com

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Finjan Software Ltd represented by **James R Hannah**
Perkins Coie LLP
101 Jefferson Dr
Menlo Park, CA 94025
650-838-4307
Email: jhannah@perkinscoie.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Lisa Kobialka
Perkins Coie LLP
101 Jefferson Dr
Menlo Park, CA 94025
650-838-4447
Email: lkobialka@perkinscoie.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Meghan Ashley Wharton
Perkins Coie LLP
101 Jefferson Dr
Menlo Park, CA 94025
650-838-4363
Email: mwharton@perkinscoie.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Paul Joseph Andre
Perkins Coie LLP
101 Jefferson Dr
Menlo Park, CA 94025
650-838-4370
Email: pandre@perkinscoie.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rachel K Zimmerman
Merchant & Gould
80 S 8th St Ste 3200
Mpls, MN 55402
(612) 332-5300
Fax: (612) 332-9081
Email:
rzimmerman@merchantgould.com

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Anthony R Zeuli
Merchant & Gould PC
80 S 8th St Ste 3200
Mpls, MN 55402
612-332-5300
Fax: 612-332-9081
Email: tzeuli@merchant-gould.com
ATTORNEY TO BE NOTICED

Defendant

Finjan Software, Inc. represented by **James R Hannah**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Lisa Kobialka
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Meghan Ashley Wharton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Paul Joseph Andre
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rachel K Zimmerman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Anthony R Zeuli
(See above for address)
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
05/04/2007	1	COMPLAINT with Jury Demand against all defendants (Filing fee $ 350 receipt number 12925.) assigned to Judge Patrick J. Schiltz per Patent List referred to Magistrate Judge Jeanne J. Graham, filed by Secure Computing Corporation. (Attachments: # 1 Civil Cover Sheet) (dch) QC'd by gjs. (Entered: 05/04/2007)

05/04/2007		Summons Issued as to Finjan Software Ltd, Finjan Software, Inc.. (dch) (Entered: 05/04/2007)
05/04/2007	2	RULE 7.1 DISCLOSURE STATEMENT by Secure Computing Corporation that there is no such parent or publicly held corporation to report. (dch) (Entered: 05/04/2007)
05/07/2007	3	ORDER OF DISQUALIFICATION. Patrick J. Schiltz recused and Magistrate Judge Jeanne J. Graham no longer assigned to case. Case reassigned to Chief Judge James M. Rosenbaum and Magistrate Judge Franklin L. Noel for all further proceedings. The new case number is 07cv2198 JMR/FLN. Signed by Judge Patrick J. Schiltz on 5/7/07. (JME) (Entered: 05/07/2007)
05/09/2007		Summons Reissued as to Finjan Software Ltd, Finjan Software, Inc.. (akl) (Entered: 05/09/2007)
05/24/2007	4	AMENDED COMPLAINT against all defendants, filed by Secure Computing Corporation. (Attachments: # 1 Certificate of Service) (Holdreith, Jacob) (Entered: 05/24/2007)
06/11/2007	5	NOTICE OF HEARING ON MOTION (Attachments: # 1 Certificate of Service)(Zeuli, Anthony) (Entered: 06/11/2007)
06/14/2007	6	MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue* by Finjan Software Ltd, Finjan Software, Inc.. (Zeuli, Anthony) (Entered: 06/14/2007)
06/14/2007	7	AMENDED NOTICE of Hearing on Motion 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue*: Motion Hearing set for 8/14/2007 09:00 AM in Minneapolis - Courtroom 15E before Chief Judge James M. Rosenbaum. (Zeuli, Anthony) (Entered: 06/14/2007)
06/14/2007	8	CERTIFICATE OF SERVICE by Finjan Software Ltd, Finjan Software, Inc. re 7 Amended Notice of Hearing on Motion, 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue* (Zeuli, Anthony) (Entered: 06/14/2007)
06/29/2007	9	MEMORANDUM in Support re 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue* filed by Finjan Software Ltd, Finjan Software, Inc.. (Attachments: # 1 LR7.1 Word Count Compliance Certificate)(Zeuli, Anthony) (Entered: 06/29/2007)
06/29/2007	10	Declaration of Ezra Sofer in Support of 9 Memorandum in Support of Motion filed by Finjan Software Ltd, Finjan Software, Inc.. (Zeuli, Anthony) (Entered: 06/29/2007)
06/29/2007	11	Declaration of Anthony R. Zeuli in Support of 9 Memorandum in Support of Motion filed by Finjan Software Ltd, Finjan Software, Inc.. (Attachments: # 1 Exhibit(s) A# 2 Exhibit(s) B# 3 Exhibit(s) C part 1# 4 Exhibit(s) C part 2# 5 Exhibit(s) C part 3# 6 Exhibit(s) C part 4# 7 Exhibit(s) D part 1# 8 Exhibit(s) D part 2# 9 Exhibit(s) D part 3)(Zeuli, Anthony) (Entered: 06/29/2007)

06/29/2007	12	RULE 7.1 DISCLOSURE STATEMENT by Finjan Software Ltd, Finjan Software, Inc. of Finjan Software, Inc. as corporate parent and/or publicly held company. (Zeuli, Anthony) (Entered: 06/29/2007)
06/29/2007	13	RULE 7.1 DISCLOSURE STATEMENT by Finjan Software, Inc. of Cisco Systems, Inc. (NASDAQ: CSCO) as corporate parent and/or publicly held company. (Zeuli, Anthony) (Entered: 06/29/2007)
06/29/2007	14	CERTIFICATE OF SERVICE by Finjan Software Ltd, Finjan Software, Inc. re 9 Memorandum in Support of Motion, 12 Rule 7.1 - Disclosure Statement, 11 Declaration in Support,, 13 Rule 7.1 - Disclosure Statement, 10 Declaration in Support (Zeuli, Anthony) (Entered: 06/29/2007)
07/23/2007	15	STIPULATION *PROTECTIVE ORDER* by Secure Computing Corporation, Finjan Software Ltd, Finjan Software, Inc.. (Attachments: # 1 Certificate of Service)(Seidl, Christopher) (Entered: 07/23/2007)
07/24/2007	16	DOCUMENT FILED IN ERROR: WILL REFILE. STIPULATION *(Amended) Protective Order* by Secure Computing Corporation, Finjan Software Ltd, Finjan Software, Inc.. (Attachments: # 1 Certificate of Service)(Seidl, Christopher) Modified text on 7/24/2007 (kt). (Entered: 07/24/2007)
07/24/2007	17	STIPULATION *(Amended) Protective Order* by Secure Computing Corporation, Finjan Software Ltd, Finjan Software, Inc.. (Attachments: # 1 Certificate of Service)(Seidl, Christopher) (Entered: 07/24/2007)
07/24/2007	18	MOTION for Admission Pro Hac Vice for Paul Joseph Andre by Finjan Software Ltd, Finjan Software, Inc.. (Zeuli, Anthony) (Entered: 07/24/2007)
07/24/2007	19	MOTION for Admission Pro Hac Vice for Lisa Kobialka by Finjan Software Ltd, Finjan Software, Inc.. (Zeuli, Anthony) (Entered: 07/24/2007)
07/24/2007	20	MOTION for Admission Pro Hac Vice for James R. Hannah by Finjan Software Ltd, Finjan Software, Inc.. (Zeuli, Anthony) (Entered: 07/24/2007)
07/24/2007	21	MOTION for Admission Pro Hac Vice for Meghan Ashley Wharton by Finjan Software Ltd, Finjan Software, Inc.. (Zeuli, Anthony) (Entered: 07/24/2007)
07/24/2007	22	STIPULATED PROTECTIVE ORDER. Signed by Judge James M. Rosenbaum on July 24, 2007. (kl) (Entered: 07/24/2007)
07/25/2007	23	MEMORANDUM in Opposition re 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue [FILED UNDER SEAL]* filed by Secure Computing Corporation. (Attachments: # 1 LR7.1 Word Count Compliance Certificate)(Foster, Trevor) RECEIVED SEALED DOCUMENT ON 7/25/07 Modified on 7/30/2007 (GJS). (Entered: 07/25/2007)

07/25/2007	24	Declaration of Paul Hawes in Support of 23 Memorandum in Opposition to Motion filed by Secure Computing Corporation. (Foster, Trevor) (Entered: 07/25/2007)
07/25/2007	25	AFFIDAVIT of Dale Ross in OPPOSITION TO 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue* filed by Secure Computing Corporation. (Foster, Trevor) (Entered: 07/25/2007)
07/25/2007	26	Declaration of Trevor J. Foster in Support of 23 Memorandum in Opposition to Motion filed by Secure Computing Corporation. (Attachments: # 1 Exhibit(s) Exs A thru G# 2 Exhibit(s) Exs H thru N# 3 Exhibit(s) Ex O, part 1# 4 Exhibit(s) Ex O, part 2# 5 Exhibit(s) Exs P thru Q# 6 Exhibit(s) Ex R, part 1# 7 Exhibit(s) Ex R, part 2# 8 Exhibit(s) Ex R, part 3# 9 Exhibit(s) Ex R, part 4# 10 Exhibit(s) Ex R, part 5# 11 Exhibit(s) Ex R, part 6# 12 Exhibit(s) Exs S thru V# 13 Placeholder for Exs W and X [Filed Under Seal])(Foster, Trevor) RECEIVED SEALED DOCUMENTS ON 7/25/07 Modified on 7/30/2007 (GJS). (Entered: 07/25/2007)
07/25/2007	27	CERTIFICATE OF SERVICE by Secure Computing Corporation re 25 Affidavit in Opposition to Motion, 24 Declaration in Support, 26 Declaration in Support,,, 23 Memorandum in Opposition to Motion (Foster, Trevor) (Entered: 07/25/2007)
07/25/2007		TEXT ONLY ENTRY - ORDER granting 18,19,20,21 Motions for Admission Pro Hac Vice of Attorneys Paul Joseph Andre, Lisa Kobialka, James R Hannah and Meghan Ashley Wharton for Finjan Software Ltd and Finjan Software, Inc. Fees paid; receipt numbers 4-014987 and 4-014988. Approved by Clerk Richard D Sletten on 7/25/07. (MMC) (Entered: 07/27/2007)
07/26/2007	28	Corrected Declaration of Trevor J. Foster in Support of 23 Memorandum in Opposition to Motion filed by Secure Computing Corporation. (Attachments: # 1 Corrected Exhibit R Part 1 of 6 # 2 Corrected Exhibit R Part 2 of 6 # 3 Corrected Exhibit R Part 3 of 6 # 4 Corrected Exhibit R Part 4 of 6 # 5 Corrected Exhibit R Part 5 of 6 # 6 Exhibit(s) R Part 6 of 6)(Foster, Trevor) Modified text on 7/26/2007 (dch). (Entered: 07/26/2007)
07/26/2007	29	CERTIFICATE OF SERVICE by Secure Computing Corporation re 28 Declaration in Support, (Foster, Trevor) (Entered: 07/26/2007)
08/02/2007	30	REPLY to Response to Motion re 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue* filed by Finjan Software Ltd, Finjan Software, Inc.. (Attachments: # 1 LR7.1 Word Count Compliance Certificate)(Zimmerman, Rachel) (Entered: 08/02/2007)
08/02/2007	31	CERTIFICATE OF SERVICE by Finjan Software Ltd, Finjan Software, Inc. re 30 Reply to Response to Motion (Zimmerman, Rachel) (Entered: 08/02/2007)
08/03/2007	32	NOTICE of Appearance by Rachel K Zimmerman on behalf of Finjan Software Ltd, Finjan Software, Inc. (Zimmerman, Rachel) (Entered:

		08/03/2007)
08/03/2007	33	CERTIFICATE OF SERVICE by Finjan Software Ltd, Finjan Software, Inc. re 32 Notice of Appearance *Rachel K. Zimmerman* (Zimmerman, Rachel) (Entered: 08/03/2007)
08/10/2007		***TEXT ONLY ENTRY*** AMENDED NOTICE of Hearing on Motion 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue*: Motion Hearing set for 8/14/2007 10:15 AM in Minneapolis - Courtroom 15E before Chief Judge James M. Rosenbaum. PLEASE NOTE CHANGE IN TIME ONLY(HLL) (Entered: 08/10/2007)
08/14/2007	34	Minute Entry for proceedings held before Chief Judge James M. Rosenbaum : Motion Hearing held on 8/14/2007 re 6 MOTION to Dismiss *or, in the Alternative, Motion to Transfer Venue* filed by Finjan Software Ltd and Finjan Software, Inc. Motion to Transfer Venue is granted. Order to be issued. (Court Reporter Dawn Hansen) (HLL) (Entered: 08/14/2007)
08/16/2007	35	ORDER granting 6 Motion to Transfer Venue to District of Delaware. Signed by Judge James M. Rosenbaum on August 15, 2007. (kl) (Entered: 08/16/2007)
10/29/2007	36	LETTER from Clerk's Office to the District of Delaware regarding transfer. (dch) (Entered: 10/29/2007)

PACER Service Center

Transaction Receipt

11/06/2007 07:37:50

PACER Login:	ud0037	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	0:07-cv-02198-JMR-FLN
Billable Pages:	4	**Cost:**	0.32

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	**Case No.** 07CV2198 PJS/JJG **COMPLAINT FOR PATENT INFRINGEMENT** **(DEMAND FOR JURY TRIAL)**

Plaintiff Secure Computing Corp. ("Secure Computing"), as and for its complaint against Defendants Finjan Software Ltd. and Finjan Software, Inc. (collectively "Finjan"), states and alleges as follows:

PARTIES

1. Plaintiff Secure Computing is a Corporation organized and existing under the laws of the State of Delaware, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

2. On information and belief, Defendant Finjan Software Ltd. is a corporation organized and existing under the laws of Israel, with its principal place of business at Harnachshev St, 1, New Industrial Area, Netanya, 42504, Israel, and its worldwide headquarters at 2025 Gateway Place, Suite 180, San Jose, California 95110.

3. On information and belief, Defendant Finjan Software, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business

SCANNED
MAY 04 2007
U.S. DISTRICT COURT MPLS

and its worldwide headquarters at 2025 Gateway Place, Suite 180, San Jose, California 95110.

JURISDICTION AND VENUE

4. This action arises under the Acts of Congress relating to patents, Title 35 U.S.C. § 1 et seq.

5. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338.

6. This Court has personal jurisdiction over Finjan because personal jurisdiction over Finjan comports with the United States Constitution, Finjan actively and regularly conducts business in the State of Minnesota and because Finjan has and continues to infringe, contributorily infringe and/or induce the infringement of U.S. Patent No. 7,171,681 in this district.

7. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b) and (c) and § 1400(b).

COUNT I
(U.S. PATENT NO. 7,171,681)

8. Plaintiff Secure Computing realleges each and every allegation set forth in Paragraphs 1 through 7, inclusive, and incorporates them herein by reference.

9. On January 30, 2007, United States Patent No. 7,171,681 ("the '681 patent") entitled "System and Method for Providing Expandable Proxy Firewall Services" issued. William E. Duncan and Vincent Hwang are the named inventors of the

'681 patent. Plaintiff Secure Computing Corporation is the assignee of the '681 patent. Plaintiff Secure Computing has been and is still the owner of the '681 patent.

10. Finjan has unlawfully infringed one or more claims of the '681 patent by making, using, offering to sell to customers, and/or selling to customers articles which infringe the claims of the '681 patent, by making, using, licensing, offering to sell and/or selling load-balancing security solutions, including but not limited to Vital Security™ Load Balancer NG-5300.

11. Finjan has engaged in activities which constitute direct infringement, contributory infringement, and/or inducement to infringe one or more claims of the '681 patent, in violation of 35 U.S.C. § 271.

12. Secure Computing has suffered damages by reason of Finjan's infringement of the '681 patent for which Secure Computing is entitled to relief under 35 U.S.C. § 284, and will suffer additional and irreparable damages unless Finjan is enjoined by this Court from continuing their infringement.

JURY DEMAND

13. A jury trial is demanded on all issues so triable, pursuant to Rule 38 of the Federal Rules of Civil Procedure and Local Rule 38.1 of the United States District Court for the District of Minnesota.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Secure Computing prays for judgment as follows:

1. That Finjan has infringed U.S. Patent No. 7,171,681;

2. That Finjan and its respective agents, servants, officers, directors, employees and all persons acting in concert with it, directly or indirectly, be enjoined from directly infringing, inducing others to infringe, and/or contributing to the infringement of U.S. Patent No. 7,171,681;

3. That Finjan be ordered to account for and pay to Plaintiff Secure Computing the damages to which Secure Computing is entitled as a consequence of the infringement of U.S. Patent No. 7,171,681;

4. That Plaintiff Secure Computing be awarded its costs and attorneys' fees herein in accordance with Title 35 United States Code § 285; and

5. That Plaintiff Secure Computing be awarded such other and further relief as the Court may deem just and equitable.

Dated: May 4, 2007

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: _____

Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (# 313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500
Counsel for Plaintiff Secure Computing Corporation

934254

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

ATTORNEYS AT LAW

2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402-2015
TEL: 612-349-8500 FAX: 612-339-4181
www.rkmc.com

Ronald J. Schutz
612-349-8435

May 4, 2007

RECEIVED
07 MAY -4 PM 3:46
CLERK'S OFFICE
MINNEAPOLIS, MN

VIA MESSENGER

Clerk of Court
United States District Court
District of Minnesota
United States Courthouse
300 South Fourth Street
Minneapolis, MN 55402

Re: *Secure Computing Corp. v. Finjan Software, Ltd., et al.*
Our File No.: 028487.0002

Dear Clerk of Court:

Enclosed for filing with respect to the above-entitled matter, please find the following documents:

1. Civil Cover Sheet;
2. Summons;
3. Complaint for Patent Infringement;
4. Rule 7.1 Disclosure Statement; and
5. Filing fee in the amount of $350.00.

Thank you for your assistance in this matter.

Very truly yours,

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

Ronald J. Schutz

RJS/cjj
Enclosures

JS 44 (Rev. 11/04)

CIVIL COVER SHEET

07cv2198

The JS-44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

I. (a) PLAINTIFFS	DEFENDANTS
Secure Computing Corp.	Finjan Software Ltd Finjan Software, Inc.
(b) County of Residence of First Listed Plaintiff Ramsey (EXCEPT IN U.S. PLAINTIFF CASES)	County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY) NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.
(c) Attorney's (Firm Name, Address, and Telephone Number) Ronald J. Schutz Jake M. Holdreith Christopher A. Seidl Trevor J. Foster Robins, Kaplan, Miller & Ciresi L.L.P. 2800 LaSalle Plaza 800 LaSalle Avenue Minneapolis, MN 55402 (612) 349-8500	Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- X 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
	PERSONAL INJURY	PERSONAL INJURY			
☐ 110 Insurance	☐ 310 Airplane	☐ 362 Personal Injury—Med. Malpractice	☐ 610 Agriculture	☐ 422 Appeal 28 USC 158	☐ 400 State Reapportionment
☐ 120 Marine	☐ 315 Airplane Product Liability	☐ 365 Personal Injury — Product Liability	☐ 620 Other Food & Drug		☐ 410 Antitrust
☐ 130 Miller Act	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 423 Withdrawal 28 USC 157	☐ 430 Banks and Banking
☐ 140 Negotiable Instrument	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	☐ 630 Liquor Laws	PROPERTY RIGHTS	☐ 450 Commerce/ICC Rates/etc.
☐ 150 Recovery of Overpayment & Enforcement of	☐ 340 Marine	☐ 370 Other Fraud	☐ 640 R.R. & Truck	☐ 820 Copyrights	☐ 460 Deportation
☐ 151 Medicare Act	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 650 Airline Regs.	X 830 Patent	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 660 Occupational Safety/Health	☐ 840 Trademark	☐ 480 Consumer Credit
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 690 Other		☐ 490 Cable/Sat TV
☐ 160 Stockholders' Suits	☐ 360 Other Personal		LABOR	SOCIAL SECURITY	☐ 810 Selective Service
☐ 190 Other Contract			☐ 710 Fair Labor Standards Act	☐ 861 HIA (1395ff)	☐ 850 Securities/Commodities Exchange
☐ 195 Contract Product Liability			☐ 720 Labor/Mgmt Relations	☐ 862 Black Lung (923)	☐ 875 Customer Challenge 12 USC 3410
			☐ 730 Labor/Mgmt Reporting & Disclosure Act	☐ 863 DIWC/DIWW (405(g))	☐ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	☐ 740 Railway Labor Act	☐ 864 SSID Title XVI	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 441 Voting	☐ 510 Motions to Vacate Sentence	☐ 790 Other Labor Litigation	☐ 865 RSI (405(g))	☐ 892 Economic Stabilization Act
☐ 220 Foreclosure	☐ 442 Employment	Habeas Corpus:	☐ 791 Empl. Ret. Inc. Security Act	FEDERAL TAX SUITS	☐ 893 Environmental Matters
☐ 230 Rent Lease & Ejectment	☐ 443 Housing/ Accommodations	☐ 530 General		☐ 870 Taxes (U.S. Plaintiff	☐ 894 Energy Allocation Act
☐ 240 Torts to Land	☐ 444 Welfare	☐ 535 Death Penalty			☐ 895 Freedom of Information Act
☐ 245 Tort Product Liability	☐ 445 Amer. w/ Disabilities Employment	☐ 540 Mandamus & Other		☐ 871 IRS—Third Party 26 USC 7609	☐ 900 Appeal of Fee Determination Under Equal Access to Justice
☐ 290 All Other Real Property	☐ 446 Amer. w/ Disabilities - Other	☐ 550 Civil Rights			☐ 950 Constitutionality of State Statues
	☐ 440 Other Civil Rights	☐ 555 Prison Condition			

V. ORIGIN (PLACE AN "X" IN ONE BOX ONLY)

X 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from another district (specify) | ☐ 6 Multidistrict Litigation | ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION

(Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 35 U.S.C. Section 1 et seq.
Brief description of cause: Patent infringement

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: X Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):
JUDGE DOCKET NUMBER

SCANNED MAY 04 2007 U.S. DISTRICT COURT MPLS

DATE 5/4/2007 SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.,

Defendants.

Case No. 07cv2198
PJS/JJG

PLAINTIFF'S RULE 7.1 DISCLOSURE STATEMENT

Plaintiff, Secure Computing Corp., states that it has no parent corporation and that no publicly-held corporation owns 10% or more of its stock.

Dated: May 4, 2007

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: _____
Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (# 313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500
Counsel for Plaintiff Secure Computing Corporation

SCANNED
MAY 04 2007
U.S. DISTRICT COURT MPLS

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION,

Plaintiff,

v.

FINJAN SOFTWARE LTD., and
FINJAN SOFTWARE, INC.,

Defendants.

Civil No. 07-CV-2198 (PJS/JJG)

ORDER OF DISQUALIFICATION

The above-captioned case has been assigned to the undersigned, a Judge of the above Court. Pursuant to Title 28, United States Code, Section 455, the undersigned recuses himself from hearing this matter. Accordingly,

IT IS ORDERED pursuant to this Court's Assignment of Cases Order filed June 29, 2006, the above-captioned action shall be resubmitted to the Clerk of Court for reassignment, and the Clerk is further directed to void and reuse a card on the Patent List of the automated case assignment system.

IT IS FURTHER ORDERED that a copy of this Order shall be filed in the above-captioned case.

Dated: May 7, 2007

s/Patrick J. Schiltz
Patrick J. Schiltz
United States District Judge

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	Case No. 0:07-cv-2198 JMR/FLN **FIRST AMENDED COMPLAINT** **(DEMAND FOR JURY TRIAL)**

Plaintiff Secure Computing Corp. ("Secure Computing"), as and for its First Amended Complaint against Defendants Finjan Software Ltd. and Finjan Software, Inc. (collectively "Finjan"), states and alleges as follows:

PARTIES

1. Plaintiff Secure Computing is a corporation organized and existing under the laws of the State of Delaware, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

2. On information and belief, Defendant Finjan Software Ltd. is a corporation organized and existing under the laws of Israel, with its principal place of business at Harnachshev St, 1, New Industrial Area, Netanya, 42504, Israel, and its worldwide headquarters at 2025 Gateway Place, Suite 180, San Jose, California 95110.

3. On information and belief, Defendant Finjan Software, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business

and its worldwide headquarters at 2025 Gateway Place, Suite 180, San Jose, California 95110.

JURISDICTION AND VENUE

4. This action arises under the Acts of Congress relating to patents, Title 35 U.S.C. § 1 et seq., Acts of Congress under § 43 of the Lanham Act, the Minnesota Deceptive Trade Practices Act, and the Minnesota common law.

5. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331, 1338, and 1367.

6. This Court has personal jurisdiction over Finjan because personal jurisdiction over Finjan comports with the United States Constitution, Finjan actively and regularly conducts business in the State of Minnesota, because Finjan has and continues to infringe, contributorily infringe and/or induce the infringement of U.S. Patent No. 7,171,681, and because Finjan has committed and continues to commit acts of unfair competition, false advertising, deceptive trade practices, and other unlawful acts, in this district.

7. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b) and (c) and § 1400(b).

COUNT I
(U.S. PATENT NO. 7,171,681)

8. Secure Computing realleges each and every allegation set forth in Paragraphs 1 through 7, inclusive, and incorporates them herein by reference.

9. On January 30, 2007, United States Patent No. 7,171,681 ("the '681 patent") entitled "System and Method for Providing Expandable Proxy Firewall Services" issued. William E. Duncan and Vincent Hwang are the named inventors of the '681 patent. Secure Computing is the assignee of the '681 patent. Secure Computing has been and is still the owner of the '681 patent.

10. Finjan has unlawfully infringed one or more claims of the '681 patent by making, using, offering to sell to customers, and/or selling to customers articles which infringe the claims of the '681 patent, by making, using, licensing, offering to sell and/or selling load-balancing security solutions, including but not limited to Vital Security™ Load Balancer NG-5300.

11. Finjan has engaged in activities which constitute direct infringement, contributory infringement, and/or inducement to infringe one or more claims of the '681 patent, in violation of 35 U.S.C. § 271.

12. Secure Computing has suffered damages by reason of Finjan's infringement of the '681 patent for which Secure Computing is entitled to relief under 35 U.S.C. § 284, and will suffer additional and irreparable damages unless Finjan is enjoined by this Court from continuing their infringement.

COUNT II
(§ 43(a) OF THE LANHAM ACT)

13. Secure Computing realleges each and every allegation set forth in Paragraphs 1 through 12, inclusive, and incorporates them herein by reference.

14. Secure Computing is in the business of developing and distributing network, systems, and web security solutions to businesses and organizations.

15. On information and belief, Finjan is in the business of developing and distributing network, systems, and web security solutions to businesses and organizations.

16. On information and belief, on March 28, 2007, Finjan distributed a worldwide press release, a copy of which continues to be posted on its company website (hereinafter "the Finjan press release").

17. The Finjan press release contains false and/or misleading statements. The Finjan press release indicates that VirusTotal.com "benchmarked [malicious] code against 32 well-known web security products." The Finjan press release states that Finjan's Vital Security Web Appliance was "the only security solution that managed to detect and block the code in real-time, without any product update or signature." The Finjan press release further states "[t]he online VirusTotal benchmark points to the superiority of our patented real-time code inspection technology."

18. The Finjan press release states that "VirusTotal is a service developed by Hispasec Sistemas, an independent IT Security laboratory."

19. On information and belief, Finjan also released a March 2007 marketing brochure entitled: "Malicious Page Under Benchmark" (hereinafter "the March 2007 marketing brochure").

20. The March 2007 marketing brochure contains false and/or misleading statements. The March 2007 marketing brochure states, in part, that "Virustotal.com benchmarked [malicious] code against 32 well-known web security products. The results, as obtained independently by VirusTotal (and not independently verified by Finjan), are republished in their entirety. . . ." The March 2007 marketing brochure further lists "Webwasher-Gateway" as a product that allegedly "**failed to detect** the code as malicious and as a result **did not block** it – meaning that businesses were still at risk."

21. On information and belief, on April 15, 2007, Hispasec Sistemas and VirusTotal.com posted an announcement on the VirusTotal.com website addressing the Finjan press release (hereinafter "the VirusTotal announcement").

22. The VirusTotal announcement stated, in part, that information related to the Finjan press release "may lead to confusion, whether that was the result intended or not, and that is why we feel compelled to declare the following at Hispasec:

- VirusTotal has not conducted any experiment or test related to AV comparative analyses.
- VirusTotal has no notice whatsoever of the malicious code [Finjan] refer[s] to in this piece of news.
- VirusTotal has never tested nor tried Finjan's security solutions."

23. The VirusTotal announcement also states that VirusTotal is not intended to be used to compare antivirus products and indicates that "[t]hose who use VirusTotal to perform AV comparative analyses should know that they are making many implicit errors in the methodology."

24. On information and belief, Finjan was notified of the VirusTotal announcement at least as early as April 17, 2007.

25. Finjan is still publishing the March 28, 2007 press release on its website.

26. Finjan, through at least the aforementioned acts described in paragraphs 14-25 including Finjan's statements regarding the alleged independent VirusTotal benchmark, and on information and belief other acts, has made false and/or misleading material statements of fact in interstate commerce that actually deceived and/or had the capacity to deceive a substantial segment of customers, in violation of § 43(a), 15 U.S.C. § 1125(a), of the Lanham Act.

27. Finjan's actual and implied misrepresentations, including at least those about the alleged independent VirusTotal benchmark, constitute unfair competition and false advertising in violation of § 43(a), 15 U.S.C. § 1125(a), of the Lanham Act.

28. Finjan's actual and implied misrepresentations are likely to influence the purchasing decisions of security product purchasers.

29. As a result of Finjan's aforementioned acts, including Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark, and unless enjoined by this Court, Secure Computing has been and will be irreparably injured by Finjan's practices described above, as to which Secure Computing has no adequate remedy at law. In addition, as a result of Finjan's foregoing acts, including Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark,

Secure Computing has been and will be damaged, in an amount to be fully determined at trial.

30. Finjan's aforementioned actions, including Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark test, were and are taken in willful, deliberate and intentional disregard of Secure Computing's rights. This case is exceptional under the Lanham Act.

COUNT III
(Minnesota Deceptive Trade Practices Act - Minn. Stat. 325D.44)

31. Secure Computing realleges each and every allegation set forth in Paragraphs 1 through 30, inclusive, and incorporates them herein by reference.

32. Finjan, through at least the aforementioned acts described in paragraphs 14-25 including Finjan's statements regarding the alleged independent VirusTotal benchmark, and on information and belief other acts, has made false and/or misleading material statements of fact in interstate commerce that actually deceived and/or had the capacity to deceive a substantial segment of security product customers, in violation of the Minnesota Deceptive Trade Practices Act (Minn. Stat. 325D.44).

33. Finjan's actual and implied misrepresentations, including at least those about the alleged independent VirusTotal benchmark, constitute unfair competition and deceptive trade practices in violation of the Minnesota Deceptive Trade Practices Act (Minn. Stat. 325D.44).

34. Finjan's actual and implied misrepresentations are likely to influence the purchasing decisions of security product purchasers.

35. Secure Computing has suffered damages by reason of Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark test, and will suffer additional and irreparable damages unless Finjan is enjoined by this Court from continuing to make and distribute false and/or misleading statements.

36. Finjan's aforementioned actions, including Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark test, were and are taken in willful, deliberate and intentional disregard of Secure Computing's rights, knowing such actions to be deceptive.

COUNT IV
(Unfair Competition and Injurious Falsehood)

37. Secure Computing realleges each and every allegation set forth in Paragraphs 1 through 36, inclusive, and incorporates them herein by reference.

38. Finjan conduct, through at least the aforementioned acts described in paragraphs 14-25 including Finjan's statements regarding the alleged independent VirusTotal benchmark, and on information and belief other acts, constitutes unfair competition and injurious falsehood under Minnesota common law.

39. As a result of Finjan's aforementioned acts, including Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark, and unless enjoined by this Court, Secure Computing has been and will be irreparably injured by Finjan's practices described above, as to which Secure Computing has no adequate remedy at law. In addition, as a result of Finjan's foregoing acts, including Finjan's false and/or misleading statements regarding the alleged independent VirusTotal benchmark,

Secure Computing has been and will be damaged, in an amount to be fully determined at trial.

JURY DEMAND

A jury trial is demanded on all issues so triable, pursuant to Rule 38 of the Federal Rules of Civil Procedure and Local Rule 38.1 of the United States District Court for the District of Minnesota.

PRAYER FOR RELIEF

WHEREFORE, Secure Computing prays for judgment as follows:

1. That Finjan has infringed U.S. Patent No. 7,171,681;

2. That Finjan and its respective agents, servants, officers, directors, employees and all persons acting in concert with it, directly or indirectly, be enjoined from directly infringing, inducing others to infringe, and/or contributing to the infringement of U.S. Patent No. 7,171,681;

3. That Finjan be ordered to account for and pay to Secure Computing the damages to which Secure Computing is entitled as a consequence of the infringement of U.S. Patent No. 7,171,681;

4. That Finjan and its respective agents, servants, officers, directors, employees and all persons acting in concert with it, directly or indirectly, be ordered to immediately take corrective action regarding Finjan's false and/or misleading statements complained of herein, including but not limited to immediately sending corrective statements in writing to all persons to whom Finjan has made the false and/or misleading

statements and to all persons who actually received the false and/or misleading statements, and placing corrective advertisements in any and all media in which it placed the false and/or misleading statements (including without limitation on its website and in all publications in which its false and/or misleading statements appeared). Such corrective statements shall run for an equal number of days as the March 28, 2007 press release appeared on Finjan's website and in the same number of publications and number of consecutive issues of the publications and in the same manner and frequency of dissemination as the offending statements appeared;

5. That Finjan and its respective agents, servants, officers, directors, employees and all persons acting in concert with it, directly or indirectly, be enjoined from publishing, disseminating, distributing, or otherwise using the representations or similar representations in the advertising and promotional materials complained of herein, including its March 28, 2007 press release and its March 2007 marketing brochure;

6. That Finjan be ordered to pay to Plaintiff Secure Computing the damages to which Secure Computing is entitled as a consequence of Finjan's false and/or misleading statements and violations of the Lanham Act, the Minnesota Deceptive Trade Practices Act, and the Minnesota common law, in an amount to be determined at trial;

7. That Plaintiff Secure Computing be awarded its costs and attorneys' fees, including costs and attorneys' fees in accordance with Title 35 United States Code § 285; Title 15 U.S.C. § 1117(a), and Minn. Stat. 325D.45;

8. That Plaintiff Secure Computing be awarded all such other relief permitted under the patent laws, the Lanham Act, the Minnesota Deceptive Trade Practices Act, and the Minnesota common law, and

9. That Plaintiff Secure Computing be awarded such other and further relief as the Court may deem just and equitable.

Dated: May 24, 2007

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: s/Jake M. Holdreith
Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (# 313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500
Counsel for Plaintiff Secure Computing Corporation

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.

Defendants.

Case No. 0:07-cv-2198 JMR/FLN

CERTIFICATE OF SERVICE

I hereby certify that on the 24th day of May, 2007, I caused the following document:

FIRST AMENDED COMPLAINT

to be filed electronically with the Clerk of Court through ECF. I further certify that I caused a copy of the foregoing document and the notice of electronic filing to be mailed via Federal Express, to the following non-ECF participants:

Paul Andre, Esq.
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114
(Counsel for Finjan Software Ltd.
Finjan Software, Inc.)

Dated: May 24, 2007

By: s/Jake M. Holdreith

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	Case No: 0:07-cv-02198-JMR-FLN

NOTICE OF HEARING ON MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that DEFENDANTS FINJAN SOFTWARE LTD. AND FINJAN SOFTWARE, INC. (collectively "Finjan"), by and through their attorneys, will move the Court to dismiss the action or, in the alternative, transfer it to another venue. The Motion will come before the Court on a date and time yet to be determined by the Court with arguments from the parties to be heard by the Honorable James Rosenbaum, U.S. District Court Judge for the District of Minnesota, Courtroom 15E, U.S. Courthouse, 300 South 4th Street, Minneapolis, Minnesota 55415.

Dated: June 11, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli
Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center
80 South Eighth Street

Minneapolis, MN 55402
Telephone: 612.332.5300
Facsimile: 612.332.9081
Email: tzeuli@merchantgould.com
Email: mailto:jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: mailto:lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

CERTIFICATE OF SERVICE

I hereby certify that on June 11, 2007, I caused the following documents:

1. **NOTICE OF HEARING ON MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE;**
2. **CERTIFICATE OF SERVICE**

to be filed electronically with the Clerk of Court through ECF, and that ECF will send an e-notice of the electronic filing to the following counsel of record:

- **Trevor J Foster**
  tjfoster@rkmc.com dgterry@rkmc.com
- **Jacob M Holdreith**
  jmholdreith@rkmc.com dgterry@rkmc.com
- **Ronald J Schutz**
  rjschutz@rkmc.com lvlind@rkmc.com;crketterling@rkmc.com
- **Christopher A Seidl**
  caseidl@rkmc.com cjjunker@rkmc.com

Dated: June 11, 2007

s/Anthony R. Zeuli
Anthony R. Zeuli

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	Case No: 0:07-cv-02198-JMR-FLN

MOTION TO DISMISS OR, IN THE ALTERNATIVE,
MOTION TO TRANSFER VENUE

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

THE DEFENDANTS FINJAN SOFTWARE LTD. AND FINJAN SOFTWARE, INC. (collectively "Finjan"), by and through their attorneys, hereby move the Court for an order dismissing Plaintiff's claims against Finjan on the grounds that the Court lacks personal jurisdiction over Finjan Software Ltd. and Finjan Software, Inc. and/or venue in this Court is improper or, in the alternative, an order transferring venue of this matter to the United States District Court for the District of Delaware. Finjan's motion is based upon Fed. R. Civ. P. 12(b)(3) and (6) and 28 U.S.C. § 1404(a).

Dated: June 14, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli
Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402

Telephone: 612.332.5300
Facsimile: 612.332.9081
Email: tzeuli@merchantgould.com
Email: jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	Case No: 0:07-cv-02198-JMR-FLN

AMENDED NOTICE OF HEARING ON MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:
TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that DEFENDANTS FINJAN SOFTWARE LTD. AND FINJAN SOFTWARE, INC. (collectively "Finjan"), by and through their attorneys, will move the Court to dismiss the action or, in the alternative, transfer it to another venue. The Motion will come before the Court on August 14, 2007 at 9:00 a.m. with arguments from the parties to be heard by the Honorable James Rosenbaum, U.S. District Court Judge for the District of Minnesota, Courtroom 15E, U.S. Courthouse, 300 South 4th Street, Minneapolis, Minnesota 55415.

Dated: June 14, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli
Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center

80 South Eighth Street
Minneapolis, MN 55402
Telephone: 612.332.5300
Facsimile: 612.332.9081
Email: tzeuli@merchantgould.com
Email: jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

CERTIFICATE OF SERVICE

I hereby certify that on June 14, 2007, I caused the following documents:

1. **MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE;**
2. **AMENDED NOTICE OF HEARING ON MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE and**
3. **CERTIFICATE OF SERVICE**

to be filed electronically with the Clerk of Court through ECF, and that ECF will send an e-notice of the electronic filing to the following counsel of record:

- **Trevor J Foster**
  tjfoster@rkmc.com dgterry@rkmc.com
- **Jacob M Holdreith**
  jmholdreith@rkmc.com dgterry@rkmc.com
- **Ronald J Schutz**
  rjschutz@rkmc.com lvlind@rkmc.com;crketterling@rkmc.com
- **Christopher A Seidl**
  caseidl@rkmc.com cjjunker@rkmc.com

Dated: June 14, 2007

s/Anthony R. Zeuli
Anthony R. Zeuli

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 2

A. The Parties. 2

B. Finjan Has Limited Contacts with Minnesota. 2

1. Finjan USA is a Delaware Corporation with its Principal Place of Business in the State of California. 2

2. Finjan Israel, a Subsidiary of Finjan USA, is an Israeli Corporation with its Principal Place of Business in Israel. 4

Substantially Similar to the Claims in the Delaware Litigation. 4

III. ARGUMENT 6

A. THIS COURT CANNOT CONSTITUTIONALLY EXERCISE PERSONAL JURISDICTION OVER FINJAN USA AND/OR FINJAN ISRAEL. 6

1. Applicable Law Regarding Motion to Dismiss Based on Lack of Personal Jurisdiction. 6

2. This Court Lacks Personal Jurisdiction over Finjan USA Because Finjan USA has Insufficient Contacts with Minnesota. 8

3. This Court Lacks Personal Jurisdiction over Finjan Israel Because Finjan Israel Has *No* Contacts with Minnesota. 12

B. THE MINNESOTA ACTION SHOULD BE DISMISSED BECAUSE VENUE IS IMPROPER IN THIS JUDICIAL DISTRICT. 14

C. IF THE MINNESOTA ACTION IS NOT DISMISSED FOR IMPROPER VENUE, VENUE SHOULD BE TRANSFERRED TO THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE. 15

1. This Court Should Transfer the Minnesota Action to the District of Delaware because Finjan Israel Filed a Similar Action in Delaware Before Secure Computing Filed the Minnesota Action and the Minnesota Action Constitutes Wasteful Parallel Litigation. 15

2. This Court Should Transfer the Minnesota Action to the District of Delaware because the District of Delaware is a More Convenient Forum for the Parties and the Witnesses. 17

3. This Court Should Transfer the Minnesota Action to the District of Delaware in the Interest of Justice and to Preserve Judicial Resources. 19

IV. CONCLUSION 20

Cases

Bell Paper Box, Inc. v. U.S. Kids, Inc., 22 F.3d 816, 818 (8th Cir. 1994) 7

Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985)..... 7, 10, 13

Coast-to-Coast Stores, Inc. v. Womack-Bowers, Inc., 594 F. Supp. 731, 734 (D. Minn. 1984). 18

Codex Corp. v. Milgo Elec. Corp., 553 F.2d 735, 739 (1st Cir. 1977) 20

Cont'l. Grain Co. v. Barge F.B.L.-585, 364 U.S. 19, 26-27 (1960))..... 15

Digi-Tel Holdings, Inc. v. Proteq Telecomm. (PTE), Ltd., 89 F.3d 519, 522 (8th Cir. 1996) ..... passim

Envtl Servs., Inc. v. Bell Lumber & Pole Co., 607 F. Supp. 851, 853 (N.D. Ill. 1984).... 17

Helicoptors Nacionales De Colombia v. Hall, 466 U.S. 408, 416 (1984) 8

Hoppe v. G.D. Searle & Co., 683 F. Supp. 1271, 1276 (D. Minn. 1988) 17

Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) 8

Kaylor v. Fields, 661 F.2d 1177, 1182 (8th Cir. 1981) 6

Lakin v. Prudential Sec., Inc., 348 F.3d 704, 711-12 (8th Cir. 2003) 12

Land-O-Nod v, Bassett Furniture Indus., Inc., 708 F.2d 1338, 1341 (D. Minn. 1994)..... 9

Morgan Distrib. Co., Inc. v. Unidynamic Corp., 868 F.2d 992, 995 (8th Cir. 1989) 6

Morris v. Barkbuster, Inc., 923 F.2d 1277, 1280 (8th Cir. 1991)). 7, 8

Reisner v. Stoller, 51 F. Supp. 2d 430, 440 (S.D.N.Y. 1999)..... 6

Sybaritic, Inc. v. Interport Int'l, Inc., 957 F.2d 522, 524 (8th Cir. 1992))..... 7, 10

Tuttle v. Lorillard Tobacco Co., 118 F. Supp. 2d 954, 959 (D. Minn. 2000); 6

West Publ'g Corp. v. Stanley, 2004 U.S. Dist. LEXIS 448, *12 (D. Minn. 2004) 6

Wilson v. Lincoln Redev. Corp., 488 F.2d 339, 341 (8th Cir. 1973) 6

Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997))..... 12

Zumbro, Inc. v. California Natural Prods., 861 F. Supp. 773, 777 (D. Minn. 1994)..... 7

Statutes

28 U.S.C. § 1391(b) 14

28 U.S.C. § 1391(b)(2) 14

28 U.S.C. § 1391(b)(3) 14

28 U.S.C. § 1391(c) 14

28 U.S.C. § 1406(a) 1, 14

28 U.S.C. § 1404(a) 1, 15

Minn. Stat. § 543.19(1)(b) 7

Rules

Fed. R. Civ. P. 12(b)(6) 1

Fed.R.Civ.P. 12(b)(3) 1, 14

Defendants Finjan Software Ltd. ("Finjan Israel") and Finjan Software, Inc. ("Finjan USA") (collectively "Finjan") submit this Memorandum of Law in Support of Defendants' Motion to Dismiss the above-captioned action for lack of personal jurisdiction pursuant to Fed. R. Civ. P. 12(b)(6) and/or improper venue pursuant to Fed. R. Civ. P. 12(b)(3) and 28 U.S.C. § 1406(a) or, in the alternative, to transfer this action to the United States District Court for the District of Delaware pursuant to 28 U.S.C. § 1404(a).

I. INTRODUCTION

This Court cannot constitutionally exercise personal jurisdiction over either Defendant in the pending action. None of the parties in this action are located in Minnesota. Plaintiff Secure Computing Corp. ("Secure Computing") and Defendant Finjan USA are Delaware corporations with their principal places of business in California. Finjan Israel is an Israeli corporation with its principal place of business in Israel. Finjan Israel has no contacts with Minnesota, and Finjan USA does not have sufficient contacts with Minnesota to warrant this Court's exercise of personal jurisdiction.

In the event this Court finds that it can exercise personal jurisdiction over Finjan USA and/or Finjan Israel, Plaintiff's Complaint should be dismissed pursuant to Fed. R. Civ. P. 12(b)(3) and 28 U.S.C. §1406(a) because venue in this judicial district is improper. In the alternative, pursuant to 28 U.S.C. § 1404(a), this action should be transferred to the United States District Court for the District of Delaware. Finjan Israel filed a patent infringement action against Secure Computing on June 5, 2006 (hereinafter the "Delaware Action"). Finjan's earlier-filed action was pending in the United States District Court for the District of Delaware when Plaintiff filed the pending action (hereinafter the "Minnesota Action"). Additionally, convenience of the parties and

witnesses favors transfer. Transfer of the case will serve the interest of justice by preserving judicial resources and avoiding the possibility of inconsistent judgments.

II. FACTUAL BACKGROUND

A. The Parties.

None of the parties in this action is located in Minnesota. Plaintiff Secure Computing is organized and existing under the laws of the State of Delaware with its corporate headquarters at 4810 Harwood Road, San Jose, California. (First Am. Compl. ¶ 1, Docket Entry No. 4 (hereinafter "Minnesota Amended Complaint".)) Secure Computing's principal place of business is in the State of California.

Defendant Finjan USA is a corporation organized and existing under the laws of the State of Delaware with its principal place of business and its worldwide headquarters at 2025 Gateway Place, Suite 180, San Jose, California 95110. (Decl. of Ezra Sofer in Supp. of Defs' Mot. to Dismiss or, in the Alternative, Mot. to Transfer Venue (hereinafter "Sofer Decl.") ¶ 1.) Defendant Finjan Israel is a corporation organized and existing under the laws of Israel, with its principal place of business at Hamachshev St. 1, New Industrial Area, Netanya, 42504, Israel. Finjan Israel is a subsidiary of Finjan USA. (Sofer Decl. ¶ 2.) Finjan is in the business of selling Internet security solutions for businesses and organizations. Secure Computing is a competitor of Finjan in the relevant marketplace. (*Id.* ¶ 3.)

B. Finjan Has Limited Contacts with Minnesota.

1. Finjan USA is a Delaware Corporation with its Principal Place of Business in the State of California.

Finjan USA is a Delaware corporation with its principal place of business in the State of California. (*Id.* ¶ 1.) Finjan USA is not licensed to do business in Minnesota and does not have offices or employees in Minnesota. (*Id.* ¶ 4.) Finjan USA has been operating in the United States since 1997, and over the past ten years, Finjan USA has

had minimal direct sales to customers in Minnesota.[1] (*Id.* ¶ 5.) In the past ten years, only four Finjan customers had a billing address in Minnesota and the total revenues generated from those sales amounted to $98,131.90 (hereinafter the "Finjan Minnesota Sales"). (*Id.* ¶ 5.) None of the Minnesota sales involve the accused product. (*Id.* ¶7.) The Finjan Minnesota Sales accounted for an insignificant portion of Finjan's worldwide revenue during this time period. (*Id.* ¶ 6.) Furthermore, Finjan USA does not advertise in publications that are specifically published in Minnesota and is unaware of soliciting business from Minnesota in any other manner. (*Id.* ¶ 8.)

Finjan USA operates a website at http://www.finjan.com ("Finjan USA Website"). On the Finjan USA website, Finjan USA makes information regarding its various products available to the general public. Finjan USA does not solicit or engage in direct commercial transactions with customers through the Finjan USA Website. The Finjan USA Website allows for a very limited exchange of information between Finjan USA and the general public in only two limited circumstances. First, members of the general public can complete and transmit a form available on the Finjan USA Website to request contact from a Finjan USA representative or a Finjan representative located in a different country. Further, by clicking a link on the Finjan USA Website, members of the general public can initiate an outgoing email addressed to Finjan. This feature of the Finjan USA Website does not generate an Internet-based communication with Finjan but rather generates an outgoing email using the operator's existing email account. This function can only be executed when the operator is accessing the Finjan USA Website using a computer that has email software associated with an active email account. (*Id.* ¶ 9.)

---

[1] Finjan USA does not track its products after they are sold to customers. (*Id.* ¶ 7.) Finjan cannot "reasonably anticipate being haled into court" in Minnesota because a customer brought Finjan's products into Minnesota. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

2. Finjan Israel, a Subsidiary of Finjan USA, is an Israeli Corporation with its Principal Place of Business in Israel.

Finjan Israel is an Israeli corporation with its principal place of business in Israel. As a foreign legal entity, Finjan Israel does not do business in the United States and is unaware of having any contact with Minnesota. It is not licensed to conduct business in Minnesota and does not have offices or employees in Minnesota. Finjan Israel is not aware of engaging in any business transactions with customers in Minnesota or in any other way soliciting business from Minnesota individuals or entities. (*Id.* ¶ 10.) The Finjan USA Website lists the Finjan Israel contact information on its "Contact Us" webpage. (*Id.* ¶ 9.)

C. The Claims in the Minnesota Action are Substantially Similar to the Claims in the Delaware Litigation.

Secure Computing filed its original complaint on May 4, 2007, which comprised of a single patent infringement cause of action. (Compl. for Patent Infringement ("Minnesota Compl."), Docket Entry No. 1.) The Complaint alleges that Finjan's product, namely Vital Security™ Load Balancer NG-5300, infringes U.S. Patent No. 7,171,681 ("the '681 patent"), entitled "System and method for providing expandable proxy firewall services." (*Id.* ¶ 9.) Notably, none of the Minnesota sales involve the accused infringing product, Vital Security™ Load Balancer NG-5300. (*Id.* ¶7.) William E. Duncan and Vincent Hwang are the named inventors of the '681 patent. (*Id.*) On its face, the '681 patent states that William E. Duncan resides in Frederick, Maryland and that Vincent Hwang resides in Potomac, Maryland. Secure Computing, a Delaware corporation, is the assignee of the '681 patent. (*Id.*)

On May 24, 2007, Secure Computing filed the Minnesota Amended Complaint, amending its original Complaint to add three additional causes of action: unfair trade practices under § 43(a) of the Lanham Act, unfair trade practices under the Minnesota Deceptive Trade Practices Act, and common law unfair competition and injurious falsehood. (Minnesota Am. Compl. ¶¶ 13-39.) Each new cause of action is based on the

allegation that Finjan's March 2007 press release and March 2007 marketing brochure allegedly (a) contained false and/or misleading statements regarding the ability of Finjan products to detect and block malicious code, and (b) listed Secure Computing's Webwasher-Gateway product among other third party products that failed to do so. (*Id.* ¶¶ 13-39.) The March 2007 press release and the March 2007 marketing brochure are posted on the Finjan Website. (*Id.)*

An earlier-filed patent infringement action has been pending between the parties in the United States District Court for the District of Delaware for more than one year (the "Delaware Action"). (Decl. of Anthony R. Zeuli in Supp. of Defs' Mot. to Dismiss or, in the Alternative, Mot. to Transfer Venue ¶ 2 ("Zeuli Decl.").) Finjan Israel initiated the action on June 5, 2006, by filing its complaint ("Finjan Delaware Complaint") against Secure Computing, Cyberguard Corporation and Webwasher AG (the latter two defendants are now wholly-owned subsidiaries of Secure Computing and are now referred to as "Secure Computing"), alleging that Secure Computing's products, including but not limited to the Webwasher suite of products, infringed and continue to infringe Finjan's U.S. Patent No. 6,092,194 ("'194 Patent"). (*Id.*) Secure Computing filed its answer and declaratory judgment counterclaims on July 26, 2006. (*Id.* ¶ 3.) On April 5, 2007, before the agreed upon deadline to amend the pleadings, Finjan Israel amended its complaint alleging that defendants have infringed and continue to infringe Finjan's U.S. Patent No. 6,804,780 ("'780 Patent") and U.S. Patent No. 7,058,822 ("'822 Patent") in addition to the '194 Patent ("Delaware Amended Complaint"). (*Id.* ¶ 4.) Secure Computing subsequently filed its answer and counterclaims on April 20, 2007, adding two counterclaims accusing Finjan Israel of infringing its U.S. Patent No. 7,185,361 ("'361 Patent") and U.S. Patent No. 6,357,010 ("'010 Patent") ("Delaware Answer and Counterclaims"). (*Id.* ¶ 5.) However, Secure Computing did not include a counterclaim for infringement of its '681 patent.

III. ARGUMENT

A. THIS COURT CANNOT CONSTITUTIONALLY EXERCISE PERSONAL JURISDICTION OVER FINJAN USA AND/OR FINJAN ISRAEL.

1. Applicable Law Regarding Motion to Dismiss Based on Lack of Personal Jurisdiction.

Pursuant to Federal Rule of Civil Procedure 12(b)(6), this case should be dismissed for lack of personal jurisdiction because Secure Computing fails to make a "prima facie showing of personal jurisdiction" over the Finjan USA and/or Finjan Israel in the Minnesota Amended Complaint. Digi-Tel Holdings, Inc. v. Proteq Telecomm. (PTE), Ltd., 89 F.3d 519, 522 (8th Cir. 1996), *see* West Publ'g Corp. v. Stanley, 2004 U.S. Dist. LEXIS 448, *12 (D. Minn. 2004). This Court must view the evidence "in the light most favorable to the plaintiff and resolve all factual conflicts in the plaintiff's favor." Digi-Tel Holdings, 89 F.3d at 522. However, "conclusory allegations or legal conclusions [made by Secure Computing] masquerading as factual conclusions [regarding jurisdiction] will not suffice to prevent a motion to dismiss." Reisner v. Stoller, 51 F. Supp. 2d 430, 440 (S.D.N.Y. 1999) (internal quotations omitted); *see also* Kaylor v. Fields, 661 F.2d 1177, 1182 (8th Cir. 1981); Wilson v. Lincoln Redev. Corp., 488 F.2d 339, 341 (8th Cir. 1973).

Further, in considering the present motion, this Court must "look[] only to the factual allegations in the complaint[as]. . . [a]ny allegations made in subsequent legal memoranda cannot correct inadequacies within a complaint." Tuttle v. Lorillard Tobacco Co., 118 F. Supp. 2d 954, 959 (D. Minn. 2000); *See* Morgan Distrib. Co., Inc. v. Unidynamic Corp., 868 F.2d 992, 995 (8th Cir. 1989) ("[I]t is axiomatic that the complaint may not be amended by the briefs in opposition to a motion to dismiss.") (internal quotations omitted).

This Court engages in a two-step process to determine whether personal jurisdiction may properly be exercised over non-resident Defendants Finjan USA and

Finjan Israel. Zumbro, Inc. v. California Natural Prods., 861 F. Supp. 773, 777 (D. Minn. 1994) (citing Morris v. Barkbuster, Inc., 923 F.2d 1277, 1280 (8th Cir. 1991)). First, this Court determines whether the exercise of personal jurisdiction over Finjan USA and/or Finjan Israel is permitted under Minnesota's long-arm statute. *Id.* Second, the Court determines whether the exercise of personal jurisdiction over Finjan USA and/or Finjan Israel by courts in Minnesota comports with constitutional due process. *Id.* Because Minnesota interprets its long-arm statute, Minn. Stat. § 543.19(1)(b), to extend personal jurisdiction to the fullest extent permitted by due process, "the inquiry collapses into a single question of whether exercising personal jurisdiction [over Finjan USA and/or Finjan Israel] comports with due process." *Id.* (citing Bell Paper Box, Inc. v. U.S. Kids, Inc., 22 F.3d 816, 818 (8th Cir. 1994) and Sybaritic, Inc. v. Interport Int'l, Inc., 957 F.2d 522, 524 (8th Cir. 1992)).

The Due Process Clause of the United States Constitution requires that this Court determine whether Finjan USA and/or Finjan Israel have sufficient "minimum contacts" with Minnesota before exercising personal jurisdiction over either Defendant. *Id.* (citing Bell Paper, 22 F.3d at 818). In order to exercise personal jurisdiction over Finjan USA and/or Finjan Israel in this matter, this Court must find that each Defendant's contact with Minnesota is more than "random," "fortuitous," or "attenuated." Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985). This Court should not exercise personal jurisdiction over Finjan USA or Finjan Israel unless it finds that Finjan USA's and/or Finjan Israel's contacts with Minnesota constitute "conduct and connection with [Minnesota] such that [either Defendant] should reasonably anticipate being haled into court" in Minnesota. World-Wide Volkswagen, 444 U.S. at 297. Jurisdiction is proper if Finjan USA's or Finjan Israel's contacts proximately result from actions that create a "substantial connection" with Minnesota. Burger King, 411 U.S. at 475. In addition to sufficient contacts, due process also requires that this Court's exercise of jurisdiction over Finjan USA and/or Finjan Israel "not offend 'traditional notions of fair play and

substantial justice.'" Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).

2. This Court Lacks Personal Jurisdiction over Finjan USA Because Finjan USA has Insufficient Contacts with Minnesota.

a. This Court Cannot Exercise General or Specific Personal Jurisdiction over Finjan based on the Finjan Minnesota Sales.

This Court cannot exercise general jurisdiction over Finjan USA unless it determines that Finjan USA maintained "continuous and systematic" contacts with the forum state, regardless of whether Secure Computing's claims are related to those contacts. Helicoptors Nacionales De Colombia v. Hall, 466 U.S. 408, 416 (1984). Finjan USA's contacts with Minnesota can in no way be characterized as "continuous and systematic." Finjan USA is not licensed to do business in Minnesota and does not have offices or employees in Minnesota. Finjan USA has had only four customers with billing addresses in Minnesota over the past 10 years. The Finjan Minnesota Sales accounted for an insignificant portion of Finjan's worldwide revenue during this time period. Such minimal relations with Minnesota entities and individuals are far short of the quantity and quality of contacts that would be considered "continuous and systematic." Secure Computing's conclusory allegation that "Finjan actively and regularly conducts business in the State of Minnesota" is without support and does not suffice to establish general jurisdiction over Finjan USA. (Minnesota Am. Compl. ¶ 6.)

As general jurisdiction is inappropriate in this matter, the personal jurisdiction question at issue is reduced to whether this Court may exercise specific jurisdiction over Finjan USA. This Court can only exercise personal jurisdiction over Finjan USA if it premises jurisdiction over Finjan USA upon the relationship between Secure Computing's claims and Finjan USA's forum state activities. Morris v. Barkbuster, Inc., 923 F.2d 1277, 1280 (8th Cir. 1991). In order to exercise specific jurisdiction over

Finjan USA, this Court must determine that the Finjan Minnesota Sales relate to Secure Computing's claims in the Minnesota Amended Complaint.

To the best knowledge of Finjan, Finjan USA's forum state activities over the past ten years are composed entirely of the Finjan Minnesota Sales. Finjan's Vital Security™ Load Balancer NG-5300 product, the only accused product identified by Secure Computing in the Minnesota Amended Complaint, was not sold in the Finjan Minnesota Sales. (Sofer Decl. ¶ 7.) Accordingly, the Finjan Minnesota Sales are unrelated to Secure Computing's patent infringement claim (Claim I of the Minnesota Amended Complaint). *See* Zumbro, 861 F.Supp. at 780 n.13 (citing Land-O-Nod v, Bassett Furniture Indus., Inc., 708 F.2d 1338, 1341 (D. Minn. 1994), and stating that "[p]romoting and selling products *not* covered by any of the patents at issue are acts *unrelated* to the subject matter of Zumbro's patent claims") (emphasis in original).

Secure Computing's trade practices claims (Claims II, III and IV of the Minnesota Amended Complaint) are similarly unrelated to the Finjan Minnesota Sales. The alleged misrepresentations are not part of any publications that are or were ever published in Minnesota or aimed at customers in Minnesota. Further, the trade practices claims assert harm to Secure Computing as a corporation. Secure Computing is not a Minnesota corporation, and any alleged harm incurred by Secure Computing as a result of Finjan USA's alleged misrepresentations will not constitute an injury to a Minnesota entity or individual. The alleged misrepresentation simply has no relation to Minnesota or the Finjan Minnesota sales. Therefore, this Court should decline to exercise specific jurisdiction over Finjan USA.

Application by this Court of the detailed analysis set out by the Eighth Circuit Court of Appeals in the Digi-Tel Holdings case will also result in the conclusion that this Court should not exercise specific jurisdiction over Finjan USA. Digi-Tel Holdings, 89 F.3d 522-23. Pursuant to Digi-Tel Holdings, this Court may examine five factors when determining whether the exercise of personal jurisdiction over Finjan USA comports with

constitutional due process: (1) the nature and quality of Finjan USA's contacts with Minnesota; (2) the quantity of Finjan's contacts with Minnesota; (3) the relation of the cause of action to Finjan USA's Minnesota contacts; (4) the interest of Minnesota in providing a forum for its residents; and (5) the convenience of the parties. *Id.* The Court of Appeals has stated that the above considerations incorporate the notions of both "minimum contacts" and "fair play and substantial justice." Sybaritic, Inc., 957 F.2d at 524.

According to the Court of Appeals, the first three of the above factors are of primary importance and can be considered together. Digi-Tel Holdings, 89 F.3d at 523. The nature and quality of Finjan USA's contacts with Minnesota are slight and tenuous and the quantity of the contacts is very limited. Such limited and tenuous contacts do not subject Finjan to the jurisdiction of this Court. Finjan USA does not have a regular business presence in Minnesota and has no offices or employees in Minnesota. Further, Finjan USA does not actively solicit business from Minnesota individuals or entities and it does not advertise its products in publications published in Minnesota. Finjan does not send its employees, product information or product samples into Minnesota. The Finjan Minnesota Sales accounted for an insignificant portion of Finjan's worldwide revenue during this time period and did not include the accused product.

Secure Computing's Minnesota Amended Complaint does not allege facts that in any way support Digi-Tel Holding's third factor. Finjan USA's limited and unrelated contacts with Minnesota do not create a "substantial connection" to Minnesota that is sufficient to justify subjecting Finjan USA to personal jurisdiction in this action. *See* Burger King, 471 U.S. at 475 (holding that jurisdiction is not proper where the contacts do not proximately result from actions by the defendant creating a "substantial connection" with the forum state). Secure Computing's causes of action in the Minnesota Amended Complaint are unrelated to Finjan USA's attenuated contacts with Minnesota. First, Finjan USA did not sell Vital Security™ Load Balancer NG-5300, the only accused

product in the pending action, in the Finjan Minnesota Sales. Second, the alleged conduct asserted by Secure Computing in support of its trade practices causes of action does not constitute contacts with Minnesota because the alleged conduct is neither aimed at customers in Minnesota nor calculated to cause injury to Minnesota residents. In summary, Finjan USA's contacts with Minnesota are insubstantial, tenuous, and fortuitous in nature and quality, and have no relation to the patent infringement claim or the trade practices claims in the Minnesota Action. As such, these contacts do not amount to the sufficient "minimum contacts" necessary to subject Finjan to the jurisdiction of this Court.

An examination of the two remaining factors addressed in the Digi-Tel Holdings opinion further exemplifies that this Court should refuse to exercise jurisdiction over Finjan USA and dismiss the Minnesota Action. First, Minnesota, the forum state, has no interest in providing a forum to Secure Computing because Secure Computing is not a Minnesota Corporation and does not have its principal place of business in Minnesota. Simply put, Minnesota has no interest in expending its limited juridical resources providing a forum for three foreign companies to litigate a dispute regarding activities that are alleged to have occurred outside Minnesota.

Finally, an analysis of the convenience of the parties strongly supports a decision by this Court that it lacks personal jurisdiction over Finjan USA. The United States District Court for the District of Delaware is a more convenient forum for all of the parties to the Minnesota Action. This is true not only for Finjan USA but also for Secure Computing and Finjan Israel. Secure Computing cannot claim that Delaware is an inconvenient forum because Secure Computing is already litigating similar claims in the District of Delaware and is incorporated in Delaware. The earlier-filed Delaware Action involves similar claims to those in the Minnesota Action. The Delaware judge has developed a working knowledge of the technology at issue.

In conclusion, the attenuated contacts that make up the Finjan Minnesota Sales do not create a "substantial connection" to Minnesota that is sufficient to subject Finjan USA to specific or general personal jurisdiction in this state.

b. This Court Cannot Exercise General or Specific Personal Jurisdiction over Finjan USA based on Finjan USA's Operation of the Finjan USA Website.

Further, Finjan USA's operation of the Finjan USA Website does not constitute sufficient contacts to support this Court's exercise of general or specific personal jurisdiction over Finjan USA. In Lakin v. Prudential Sec., Inc., 348 F.3d 704, 711-12 (8th Cir. 2003), the Eighth Circuit identified the test for determining whether a court has general or specific jurisdiction over a case involving Internet activities asserted as forum state contacts. In Lakin, the Court stated that "[a] passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise [of] personal jurisdiction." *Id.* at 710-11 (quoting Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997)). The alleged contact in the Lakin matter involved "a sophisticated interactive Web site in which a user. . . [can] establish and access secure online accounts; [] calculate home mortgage rates [and] complete online applications for home-equity loans and lines of credit." Considering these Internet activities, the Lakin court determined that such contacts alone were insufficient for a finding of general jurisdiction. Lakin, 348 F.3d at 712. The Finjan USA Website provides for substantially less interaction with the general public than the website that was at issue in the Lakin matter. Therefore, under Lakin, this Court cannot justify the exercise general or specific personal jurisdiction over Finjan USA based on its limited Internet activities involving the Finjan USA Website.

3. This Court Lacks Personal Jurisdiction over Finjan Israel Because Finjan Israel Has *No* Contacts with Minnesota.

This Court also lacks personal jurisdiction over Finjan Israel. Finjan Israel has no contacts with Minnesota. Finjan Israel is an Israeli corporation with its principal place of

business in Israel. Finjan Israel is not licensed to conduct business in any state, including Minnesota. As a foreign entity, Finjan Israel is unaware of ever having any contact with any individual or entity residing in Minnesota. Finjan Israel does not have offices or employees in Minnesota nor is Finjan Israel aware of having engaged in any business transactions with entities or individuals residing in Minnesota or in any other way soliciting business from Minnesota residents. Therefore, there is no basis upon which this Court may exercise personal jurisdiction over Finjan Israel.

In the event this Court finds that it may exercise personal jurisdiction over Finjan USA, the Court should treat Finjan Israel as a separate and independent entity and grant its motion to dismiss for lack of personal jurisdiction. Finjan Israel, as a foreign corporation, has no contact with Minnesota, and Finjan USA's contacts with Minnesota, including the operation of the Finjan USA Website, cannot be imputed to Finjan Israel. In Digi-Tel Holdings, a case with a similar factual pattern, the 8th Circuit rejected the plaintiff's argument that the defendant's parent company's activities should be imputed to the defendant. 89 F.3d at 523-524 (citing Burger King, 471 U.S. at 480 n. 22 and holding that evidence that defendant's parent company applied for a Minnesota copyright and sent two representatives to visit the plaintiff in Minnesota was not sufficient evidence to support an inference that the parent company's activities were "directed by or primarily for the benefit of" the subsidiary).

Digi-Tel Holdings applies in this action. Even though Finjan Israel is a subsidiary of Finjan USA, Finjan Israel is a separate legal entity incorporated and operating in Israel. In the Minnesota Amended Complaint, Secure Computing simply ignores Finjan Israel's separate legal entity status and does not assert evidence to support an inference that Finjan USA's minimal Minnesota contacts were directed by or primarily for the benefit of Finjan Israel. Accordingly, the Court cannot impute Finjan USA's contacts with Minnesota to Finjan Israel in determining whether it has personal jurisdiction over Finjan Israel. Since Finjan Israel has no contacts with Minnesota, the Court has no

personal jurisdiction over Finjan Israel and should grant Finjan Israel's motion to dismiss for lack of personal jurisdiction.

B. THE MINNESOTA ACTION SHOULD BE DISMISSED BECAUSE VENUE IS IMPROPER IN THIS JUDICIAL DISTRICT.

If this Court does not dismiss the claims asserted against either defendant for lack of personal jurisdiction, Finjan hereby moves this Court to dismiss the pending action pursuant to Fed. R. Civ. P. 12(b)(3). Pursuant to Fed. R. Civ. P. 12 (b)(3) and 28 U.S.C. § 1406(a), the Minnesota Action should be dismissed because venue in this Court is improper. Under 28 U.S.C. § 1391(b)(2) and (3), venue for the pending action must be in a judicial district in which "a substantial part of the events or omissions giving rise to the claim occurred" or "in which any defendant may be found, if there is no district in which the action may otherwise be brought." [5] As discussed in detail above, no part of the events or omissions allegedly giving rise to Secure Computing's claims occurred in Minnesota. Therefore, venue is only appropriate in Minnesota if this Court determines that Finjan USA and/or Finjan Israel *reside* in Minnesota.

Under 28 U.S.C. § 1391(c), Finjan USA and Finjan Israel are deemed to *reside* in any judicial district in which they were individually subject to personal jurisdiction at the time Secure Computing commenced the action. Consequently, a finding of proper venue for the present action in Minnesota is contingent upon the establishment of this Court's ability to constitutionally exercise personal jurisdiction over Finjan USA and/or Finjan Israel. As explained in the previous argument, this Court lacks personal jurisdiction over Finjan USA and/or Finjan Israel, and therefore venue in the Minnesota Action is improper under 28 U.S.C. § 1391(c).

---

[5] Subsection (b) of § 1391 is applicable in this matter because this Court's jurisdiction is based on a federal question and not solely on diversity of citizenship. 28 U.S.C. § 1391(b). Because Finjan Israel and Finjan USA reside in different judicial districts, 28 U.S.C. § 1391(b)(1) is not applicable in this matter.

C. IF THE MINNESOTA ACTION IS NOT DISMISSED FOR IMPROPER VENUE, VENUE SHOULD BE TRANSFERRED TO THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE.

If this Court does not dismiss the Minnesota action for improper venue, Finjan requests that this Court transfer the pending action to the United States District Court for the District of Delaware pursuant to 28 U.S.C. § 1404(a). As described above, a related action filed by Defendant Finjan Israel is currently pending in the District of Delaware. Because the criteria of Section 1404(a) strongly favor resolution of the Minnesota Action in the District of Delaware, this Court should exercise its discretion to transfer this action to the District of Delaware. This Court has discretionary authority to transfer the pending action to the District of Delaware. Under 28 U.S.C. § 1404(a), "[f]or the convenience of the parties and witnesses, [and] in the interest of justice, a district court may transfer any civil action to any other district or division where it might have been brought." The purpose of Section 1404(a) "is to prevent the waste 'of time, energy and money' and 'to protect litigants, witnesses and the public against unnecessary inconvenience and expense.'" Van Dusen v. Barrack, 376 U.S. 612, 616 (1964) (quoting Cont'l. Grain Co. v. Barge F.B.L.-585, 364 U.S. 19, 26-27 (1960)).

In considering Finjan's request to transfer venue under 28 U.S.C. § 1404(a), the court considers three factors: "(1) the convenience of the parties, (2) the convenience of the witnesses, and (3) the interests of justice." Terra Int'l, Inc. v. Miss. Chem. Corp., 119 F.3d 688, 691 (8th Cir. 1997).

1. This Court Should Transfer the Minnesota Action to the District of Delaware because Finjan Israel Filed a Similar Action in Delaware Before Secure Computing Filed the Minnesota Action and the Minnesota Action Constitutes Wasteful Parallel Litigation.

In the Delaware Action, Finjan Israel asserts claims directly related to the patents and factual allegations presented by Secure Computing in the Minnesota Action. Finjan Israel's earlier-filed action should be given priority by this Court because Secure Computing's action constitutes parallel litigation pending before a different federal court.

Under such circumstances, the action first filed is given priority for purposes of establishing venue. *See* Northwest Airlines, Inc. v. Am. Airlines, Inc., 989 F.2d 1002, 1006 (8th Cir. 1993) ("To conserve judicial resources and avoid conflicting rulings, the first-filed rule gives priority, for purposes of choosing among possible venues when parallel litigation has been instituted in separate courts, to the party who first establishes jurisdiction.")

Finjan Israel's earlier-filed Delaware Action has priority over the Minnesota Action. First, the Delaware Action and the Minnesota Action have two common parties. Secure Computing and Finjan Israel are parties in both actions. As a plaintiff in the Delaware Action, Finjan Israel submitted itself to the jurisdiction of Delaware. As such, Secure Computing will not face a personal jurisdiction issue if it asserts its claims against Finjan Israel as counterclaims in the Delaware Action.

Second, both actions involve patent infringement claims. In the Delaware Action, Finjan Israel accused Secure Computing of infringing its '194, '788 and '820 patents. Secure Computing counterclaimed by accusing Finjan Israel of infringing its '361 and '010 patents. In the Minnesota Action, Secure Computing accused Finjan Israel and Finjan USA of infringing its '681 patent. It is undisputable that all of the patents at issue in the two actions relate to technology providing Internet security to customers – a market in which Finjan and Secure Computing directly compete for customers. (Sofer Decl. ¶ 3.)

Third, even though Secure Computing added three trade practices related causes of action in its Minnesota Amended Complaint, the product that is allegedly harmed by the alleged misrepresentations is Secure Computing's Webwasher product, which is indeed the key accused infringing product in the Delaware action.

There is significant overlapping and similarity between the two actions and it would be an unnecessary use of judicial resources to allow the actions to proceed in

parallel in two different federal courts. Therefore, to preserve judicial resources, this Court should transfer the Minnesota Action to the District of Delaware.

2. This Court Should Transfer the Minnesota Action to the District of Delaware because the District of Delaware is a More Convenient Forum for the Parties and the Witnesses.

This Court should transfer the Minnesota Action to the District of Delaware for the convenience of the parties. The Eighth Circuit Court of Appeals, in Terra Int'l, Inc., sets forth a test to evaluate the convenience component in evaluating a change of venue request. 119 F.3d at 696 (8th Cir. 1997). In analyzing the convenience component, this Court should consider (1) the convenience of the parties, (2) the convenience of the witnesses – including the willingness of witnesses to appear, the ability of this Court to subpoena witnesses, and the adequacy of deposition testimony, (3) the parties' accessibility to records and documents." *Id.* This Court may also consider other factors such as the location where the alleged offending conduct occurred, and any relevant differences between Minnesota and Delaware state substantive law. *Id.*

The unique factual circumstances now before this Court present a situation where the normal presumption in favor of a plaintiff's choice of forum is not in the best interest of the parties. Therefore, this Court should address the venue question by making an examination of the "net inconvenience" to the parties. Graff v. Qwest Communications Corp., 33 F. Supp. 2d 1117, 1121 (D. Minn. 1999). Furthermore, because Minnesota lacks significant contact with the cause of action, Secure Computing's choice of forum has "reduced value." Envtl. Servs., Inc. v. Bell Lumber & Pole Co., 607 F. Supp. 851, 853 (N.D. Ill. 1984). Secure Computing's choice of Minnesota as the forum for adjudicating its claims against Finjan is just one of the many factors this Court should consider when making its determination of convenience. Hoppe v. G.D. Searle & Co., 683 F. Supp. 1271, 1276 (D. Minn. 1988).

As discussed in detail above, none of the parties reside in Minnesota, and Minnesota has minimal interest in the causes of action presented in the Minnesota Amended Complaint. Simply by looking at the locations of the parties' states of incorporation and operation, it is clear that having the action tried in Minnesota is not convenient to any party. In contrast, Delaware is a convenient forum for all of the parties because Secure Computing and Finjan USA are both incorporated in Delaware and Finjan Israel has submitted to the jurisdiction of Delaware Courts.

This Court should strongly consider that Delaware is a much more convenient forum for the litigation of the claims in the pending action. **"**The convenience of the witnesses is an important factor for the court since it determines the 'relative ease of access to sources of proof.'" Graff, 33 F. Supp. 2d at 1121, citing Gulf Oil Corp. v. Gilbert, 330 U.S. 501, 508 (1947). Important to this Court's analysis of this issue is the number of essential non-party witnesses, the location of these witnesses and the Courts' preference for live testimony over depositions. Coast-to-Coast Stores, Inc. v. Womack-Bowers, Inc., 594 F. Supp. 731, 734 (D. Minn. 1984).

In reviewing the claims in the present action, it is clear that the key factual witnesses for Secure Computing's patent infringement claim will be the inventors of the '681 Patent and the current or former employees of Finjan who participated in the development of the accused product, Vital Security™ Load Balancer NG-5300. The inventors of the patent-in-suit live in Maryland, a state sharing a border with Delaware. Therefore, it would clearly be more convenient to the inventors to have the case tried in Delaware. As for the Finjan employees who developed the accused product, further investigation will likely show that several of these individuals have left Finjan and are not subject to this Court's subpoena power for testimony at trial or taking deposition. In fact, many of these individuals currently reside in other countries. With the case transferred to Delaware would be in a better position to arrange for former employees to attend depositions or testify at trial.

This court should also consider the other Terra Int'l factors such as accessibility to records and documents, location where the alleged offending conduct occurred, and any relevant differences between Minnesota and Delaware state substantive law. 119 F.3d at 696. Since Delaware is where Secure Computing and Finjan USA are both incorporated, key business documents for these entities will be located in Delaware. To the extent Secure Computing was injured by Finjan's alleged improper conduct, that injury occurred in either California (location of Secure Computing's headquarters) or in Delaware (Secure Computing's state of incorporation).

Further, Secure Computing's patent infringement and Lanham Act claims will be analyzed under the federal statutory and common law. Secure Computing's Minnesota Deceptive Trade Practices Act will be analyzed using the principles established for Lanham Act claims. *See* Rainbow Play Sys., Inc. v. GroundScape Tech., LLC., 364 F. Supp. 2d 1026, 1039 (D. Minn. 2005) (stating that deceptive trade practice and false advertising claims under Minnesota law require the same analysis as similar claims under federal Lanham Act). In examining each of the above additional factors, this Court must find that the analysis favors transfer of the Minnesota Action to the District of Delaware.

3. This Court Should Transfer the Minnesota Action to the District of Delaware in the Interest of Justice and to Preserve Judicial Resources.

In determining whether venue should be transferred, this court should place substantial weight on fact that transfer to the District of Delaware is in the interest of justice and will preserve judicial resources. Radisson Hotels Int'l, Inc. v. Westin Hotel Co., 931 F. Supp. 638, 641 (D. Minn. 1996). Among the considerations weighed under this factor, judicial economy looms large in this case. Terra Int'l, 119 F.3d at 696.

Judicial economy would be best served by this Court transferring venue to the District of Delaware. Judicial economy is served by allowing related actions to proceed in the same district. 17 Moore's Federal Practice § 111.13[1][o]. The earlier-filed patent litigation in Delaware has common parties, involves patent infringement claims relating

to similar technology, and relates to the same products as the Minnesota action. This Court should give great weight to the fact that the District of Delaware has presided over a very similar case for almost a year and has obtained substantial familiarity with both the technology related to the patent infringement claims and the industry in which Secure Computing and Finjan compete. Allowing related actions to proceed in the District of Delaware will undoubtedly promote judicial economy. Accordingly, this Court should transfer the present case to Delaware.

Judicial economy would also be served by avoiding duplicative parallel litigation. Houk v. Kimberly-Clark Corp., 613 F. Supp. 923, 931 (W.D. Mo. 1985); *see* Codex Corp. v. Milgo Elec. Corp., 553 F.2d 735, 739 (1st Cir. 1977) ("The pendency of related litigation in another forum is a proper factor to be considered in resolving choice of venue questions.").

IV. CONCLUSION

Defendants Finjan USA and Finjan Israel respectfully request that this Court dismiss the pending action for lack of personal jurisdiction. The Complaint does not (and the Plaintiff cannot) allege sufficient contacts between Finjan USA and/or Finjan Israel and the State of Minnesota to support this Court's exercise of jurisdiction over either entity.

In the event the Court determines that all jurisdictional requirements have been satisfied over Finjan USA and/or Finjan Israel, this Court should dismiss the pending action for improper venue. In the alternative, this Court should transfer the action to the United States District Court for the District of Delaware for the convenience of the parties and witnesses and to preserve judicial resources.

Dated: June 29, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli

Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
Telephone: 612.332.5300
Facsimile: 612.332.9081
Email: tzeuli@merchantgould.com
Email: jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 7.1

Anthony Zeuli, attorney for Defendants, certifies that the "Memorandum of Law in Support of Defendants' Motion to Dismiss for Lack of Personal Jurisdiction or, in the Alternative, Motion to Transfer Venue" complies with the length limitation and type size limitation of Local Rule 7.1. The Memorandum of Law is created in Microsoft Word software and pursuant to the word count function of this software, there are 6521 words in the document, inclusive of all footnotes, and that said document is 21 pages in length.

Dated: June 29, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli

Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
Telephone: 612.332.5300
Facsimile: 612.332.9081

Email: tzeuli@merchantgould.com
Email: mailto:jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: mailto:lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Case No: 05-2448 ADM/AJB

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.,

Defendants.

DECLARATION OF EZRA SOFER IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE

I, EZRA SOFER, declare:

I am currently the CFO of Finjan Software Ltd. and Finjan Software, Inc. (collectively referred to as "Finjan"). I have held this position since January 2007. I am over 18 years of age. As part of my duties and responsibilities as CFO of Finjan, I am knowledgeable about Finjan's operations and business. If called to testify, I would and could competently testify regarding the following matters:

1. Finjan Software, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business and its worldwide headquarters at 2025 Gateway Place, Suite 180, San Jose, California 95110, United States of America (hereinafter referred to as "Finjan USA").

2. Finjan Software Ltd. is a corporation organized and existing under the laws of Israel, with its principal place of business at Hamachshev St. 1, New Industrial Area, Netanya, 42504, Israel (hereinafter referred to as "Finjan Israel"). Finjan Israel is a subsidiary of Finjan USA.

3. Finjan is in the business of selling Internet security solutions for businesses and organizations. Secure Computing is a competitor of Finjan in the relevant marketplace.

E.S.

4. Finjan USA is not licensed to do business in Minnesota and does not have offices or employees in Minnesota.

5. Finjan USA has been operating in the United States since 1997, and over the past ten years, Finjan USA has had minimal direct sales to customers in Minnesota. In the past ten years, only four Finjan customers had a billing address in Minnesota and the total revenues generated from those sales amounted to $98,131.90 (hereinafter the "Finjan Minnesota Sales").

6. The Finjan Minnesota Sales accounted for an insignificant portion of Finjan's worldwide revenue during this time period.

7. Finjan did not sell the accused infringing product, Vital Security™ Load Balancer NG-5300 to any individual or entity in Minnesota. Finjan USA does not track its products after they were sold to its customers.

8. Finjan USA does not advertise in publications that are specifically published in Minnesota, is unaware of sending product information or product samples directly to persons or entities located in Minnesota, and is unaware of soliciting business from Minnesota in any other manner.

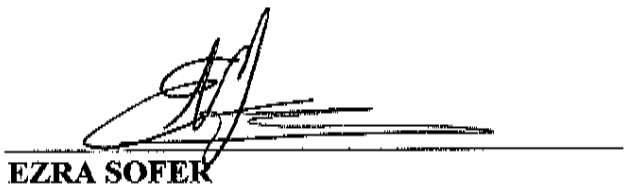
9. Finjan USA operates a website at http://www.finjan.com ("Finjan USA Website"). On the Finjan USA website, Finjan USA makes information regarding its various products available to the general public. Finjan USA does not solicit or engage in direct commercial transactions with customers through the Finjan USA Website. The Finjan USA Website allows for a very limited exchange of information between Finjan USA and the general public. The Finjan Website allows for the exchange of information between Finjan and the members of the general public in only two limited circumstances. First, members of the general public can complete and transmit a form available on the Finjan USA Website to request contact from a Finjan USA representative or a Finjan representative located in a different country. Further, by clicking a link on the Finjan USA Website, members of the general public can initiate an outgoing email addressed Finjan USA. This feature of the Finjan USA Website does not generate an Internet based communication with Finjan but rather generates an outgoing email

E.S.

using the operator's existing email account. This function can only be executed when the operator is accessing the Finjan USA Website using a computer that has email software associated with an active email account. The Finjan USA Website lists the Finjan Israel contact information on its "Contact Us" webpage.

10. Finjan Israel is an Israeli corporation with its principal place of business in Israel. As a foreign legal entity, Finjan Israel is unaware of having any contact with Minnesota. It is not licensed to conduct business in Minnesota and does not have offices or employees in Minnesota. Finjan Israel is not aware of engaging in any business transactions with customers in Minnesota or in any other way soliciting business from Minnesota individuals or entities.

I declare under penalty of perjury that the foregoing is true and correct and that this affidavit was executed pursuant to the laws of the United States on June 7, 2007, in New York, USA.



EZRA SOFER

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

DECLARATION OF ANTHONY R. ZEULI IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE

I, Anthony R. Zeuli, declare as follows:

1. I am an attorney at the law firm of Merchant & Gould P.C., counsel of record for Defendants Finjan Software, Inc. ("Finjan USA") and Finjan Software Ltd. ("Finjan Israel") in the above-referenced matter. I have personal knowledge of the following facts and, if called upon to testify, I could and would testify competently thereto.

2. There is a pending patent infringement action between Secure Computing Corp. and Finjan Israel. in the District Court of Delaware. Finjan Israel initiated the action on June 5, 2006, by filing a complaint against Secure Computing, Cyberguard Corporation and Webwasher AG (the latter two defendants are wholly-owned subsidiaries of Secure Computing)(collectively referred to as "Secure Computing"), alleging that Secure Computing has infringed and continues to infringe Finjan's U.S. Patent No. 6,092,194 ("'194 Patent"). Attached hereto as Exhibit A is a true and correct copy of the Complaint filed by Finjan Israel. on June 5, 2006 with the United States District Court of Delaware, entitled Finjan Software Ltd. v. Secure Computing Corp, with Case No. -6-369 (the "Delaware Action").

3. Secure Computing filed its answer and declaratory judgment counterclaims on July 26, 2006. Attached hereto as Exhibit B is a true and correct copy of the Answer and Counterclaims.

4. On April 5, 2007, Finjan Israel amended its complaint and added two more patent infringement claims, alleging that defendants have infringed and continue to infringe Finjan's U.S. Patent No. 6,804,780 ("'780 Patent") and U.S. Patent No. 7,058,822 ("'822 Patent") in addition to the '194 Patent. Attached hereto as Exhibit C is a true and correct copy of the Amended Complaint.

5. Secure Computing subsequently filed its answer and counterclaims on April 20, 2007. While still alleging declaratory judgment counterclaims against Finjan Israel, Secure Computing also asserted two counterclaims, accusing Finjan Israel of infringing its U.S. Patent No. 7,185,361 ("'361 Patent")and U.S. Patent No. 6,357,010 ("'010 Patent"). Attached hereto as Exhibit D is a true and correct copy of the Answer and Counterclaims.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on June 29, 2007

s/Anthony R. Zeuli
Anthony R. Zeuli

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation,	)	
Plaintiff,	)	Civil Action No.
v.	)	
SECURE COMPUTING CORPORATION, a Delaware corporation; CYBERGUARD CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100,	)	**DEMAND FOR JURY TRIAL**
Defendants.	)	

Plaintiff Finjan Software, Ltd. ("Plaintiff" or "Finjan") alleges as follows:

THE PARTIES

1. Plaintiff Finjan is a corporation organized and existing under the laws of Israel, with its principal place of business at Hamachshev St. 1, New Industrial Area, Netanya, 42504, Israel.

2. On information and belief, Defendant Secure Computing Corporation ("Secure Computing") is a corporation organized and existing under the laws of the State of Delaware, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

3. On information and belief, Defendant Cyberguard Corporation ("Cyberguard") is a corporation organized and existing under the laws of the State of Delaware and a wholly owned subsidiary of Secure Computing, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

4. On information and belief, Defendant Webwasher AG ("Webwasher") is corporation organized and existing under the laws of Germany and a wholly owned subsidiary of Cyberguard, with a branch office at 5201 Great America Parkway, Suite 432, Santa Clara, CA 95054.

JURISDICTION AND VENUE

5. This action arises under the Patent Act, 35 U.S.C. §271 *et seq*. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§1331 and 1338.

6. Venue in this judicial district is proper under 28 U.S.C. §§ 1391 (b) and (c) and/or 28 U.S.C. § 1400(b). Personal jurisdiction over defendants comports with the United Stats Constitution and § 3104 of the Delaware Code because defendants are Delaware corporations and/or have and continue to infringe, contributorily infringe and/or induce the infringement of U.S. Patent No. 6,092,194 in this district.

PLAINTIFF'S PATENT

7. On July 18, 2000, United States Patent No. 6,092,194 ("the '194 Patent"), entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, was issued to Shlomo Touboul. Finjan was assigned all ownership rights to the '194 Patent. A true and correct copy of the '194 Patent is attached to this complaint as Exhibit A and is incorporated by reference herein.

8. The '194 Patent is directed to a system and method for protecting networks and computers from hostile downloadable executable application programs.

PATENT INFRINGEMENT

9. On information and belief, defendant Secure Computing is in the business of developing and distributing network and systems security solutions to organizations. Secure

Computing has and continues to infringe the '194 Patent by making, using, selling, distributing, advertising and marketing products, including but not limited to the Webwasher Secure Content Management ("SCM") suite, that infringe the '194 Patent.

10. On information and belief, defendant Cyberguard is in the business of developing and distributing information security solutions. Cyberguard has and continues to infringe the '194 Patent by making, using, selling, distributing, advertising and marketing products, including but not limited to the Webwasher Secure Content Management ("SCM") suite, that infringe the '194 Patent.

11. On information and belief, defendant Webwasher is in the business of developing and distributing Internet and email content security and filtering solutions. Webwasher has and continues to infringe the '194 Patent by making, using, selling, distributing, advertising and marketing products, including but not limited to the Webwasher Secure Content Management ("SCM") suite, that infringe the '194 Patent.

FIRST CAUSE OF ACTION

(Infringement of the '194 Patent)

12. Finjan realleges each and every allegation set forth in Paragraphs 1 through 11, inclusive, and incorporates them herein by reference.

13. Defendants Secure Computing, Cyberguard and Webwasher have been and continue to infringe, contributorily infringe, and/or induce the infringement of the '194 Patent by making, using, selling and/or offering to sell products which infringe the '194 Patent, including but not limited to the Webwasher SCM suite, and will continue to do so until enjoined by this Court.

14. Defendants' infringement of the '194 Patent has been and continues to be willful and deliberate.

14. Defendants' infringement of the '194 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Finjan prays that the Court grant the following relief and judgment:

A. A preliminary and permanent injunction against Defendants Secure Computing, Cyberguard and Webwasher and its respective officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing, contributorily infringing, or inducing the infringement of the '194 Patent, and for all further and proper injunctive relief pursuant to 35 U.S.C. §283;

B. An award to Finjan of such damages as it shall prove at trial against Defendants Secure Computing, Cyberguard and Webwasher, that are adequate to fully compensate it for their infringement of the '194 Patent, said damages to be no less than a reasonable royalty;

C. An award to Finjan for willful infringement against Defendants Secure Computing, Cyberguard and Webwasher of three times the damages so determined, as provided by 35 U.S.C. §284, together with prejudgment interest from the date infringement of the '194 Patent began;

D. A finding that this case is "exceptional" and an award to Finjan of its costs and reasonable attorney's fees, as provided by 35 U.S.C. §285;

E. Such further and other relief as the Court and/or jury may deem proper and just.

DEMAND FOR JURY TRIAL

Plaintiff Finjan Software, Ltd. hereby demands a trial by jury on all issues triable by a jury.

POTTER ANDERSON & CORROON LLP

By _____

Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

OF COUNSEL

Paul J. Andre
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, California 94025-1114
(650) 838-4300

Dated: June 5, 2006

734999

EXHIBIT A

US006092194A

United States Patent [19]

Touboul

[11] Patent Number: 6,092,194

[45] Date of Patent: *Jul. 18, 2000

[54] **SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES**

[75] Inventor: **Shlomo Touboul**, Kefar-Haim, Israel

[73] Assignee: **Finjan Software, Ltd.**, Netanya, Israel

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/964,388**

[22] Filed: **Nov. 6, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/030,639, Nov. 8, 1996.

[51] **Int. Cl.**[7] **H04L 1/00**

[52] **U.S. Cl.** **713/200**

[58] **Field of Search** 395/187.01, 186; 713/200, 201, 202; 714/38, 704; 709/229

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,077,677	12/1991	Murphy et al.	395/10
5,361,359	11/1994	Tajalli et al.	395/700
5,485,409	1/1996	Gupta et al.	395/186
5,485,575	1/1996	Chess et al.	395/183.14
5,572,643	11/1996	Judson	395/793
5,623,600	4/1997	Ji et al.	395/187.01
5,638,446	6/1997	Rubin	380/25
5,692,047	11/1997	McManis	380/4
5,692,124	11/1997	Holden et al.	395/187.01
5,720,033	2/1998	Deo	395/186
5,724,425	3/1998	Chang et al.	380/25
5,740,248	4/1998	Fieres et al.	380/25
5,761,421	6/1998	van Hoff et al.	395/200.53
5,765,205	6/1998	Breslau et al.	711/203
5,784,459	7/1998	Devarakonda et al.	380/4
5,796,952	8/1998	Davis et al.	395/200.54
5,805,829	9/1998	Cohen et al.	395/200.32
5,832,208	11/1998	Chen et al.	395/187.01
5,850,559	12/1998	Angelo et al.	395/750.03
5,864,683	1/1999	Boebert et al.	395/200.79
5,892,904	4/1999	Atkinson et al.	395/187.01

OTHER PUBLICATIONS

Web page: http://iel.ihs.com:80/cgi-bin/iel_cgi?se...2chts%26ViewTemplate%3ddocvie%5fb%2chts, Okamato, E. et al., "ID-Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013-5194, Jul. 19, 1990, Abstract and pp. 1169-1170

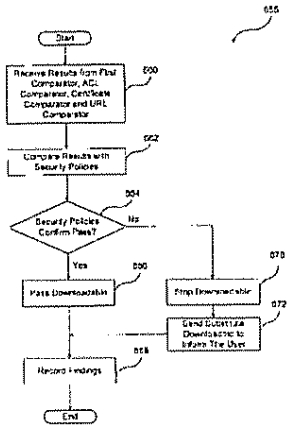
(List continued on next page.)

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Christopher Revak
Attorney, Agent, or Firm—Graham & James LLP

[57] **ABSTRACT**

A system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

68 Claims, 10 Drawing Sheets



www.freepatentsonline.com

OTHER PUBLICATIONS

"Finjan Announces a Personal Java ™ Firewall For Web Browsers—the SurfinShield™ 1 6", Press Release of Finjan Releases SurfinShield, Oct 21, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software, Ltd , Jul 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™"Article published on the Internet by Finjan Software Ltd , 1996, 2 Pages

"Company Profile Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd , Oct 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2 0" Las Vegas Convention Center/Pavillion 5 P5551, Nov 18, 1996, 3 pages

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd , 1996, 8 pages

"Products" Article published on the Internet, 7 pages

Mark LaDue, "Online Business Consultant" Article published on the Internet, Home Page, Inc 1996, 4 pages

Jim K Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, p 27, May 1990

Norvin Leach et al, "IE 3 0 applets will earn certification", PC Week, v13, n29, p1(2), Jul 1996

Microsoft Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct 1996

Frequently Asked Questions About Authenticode, Microsoft Corporation, Feb 1997

www.freepatentsonline.com

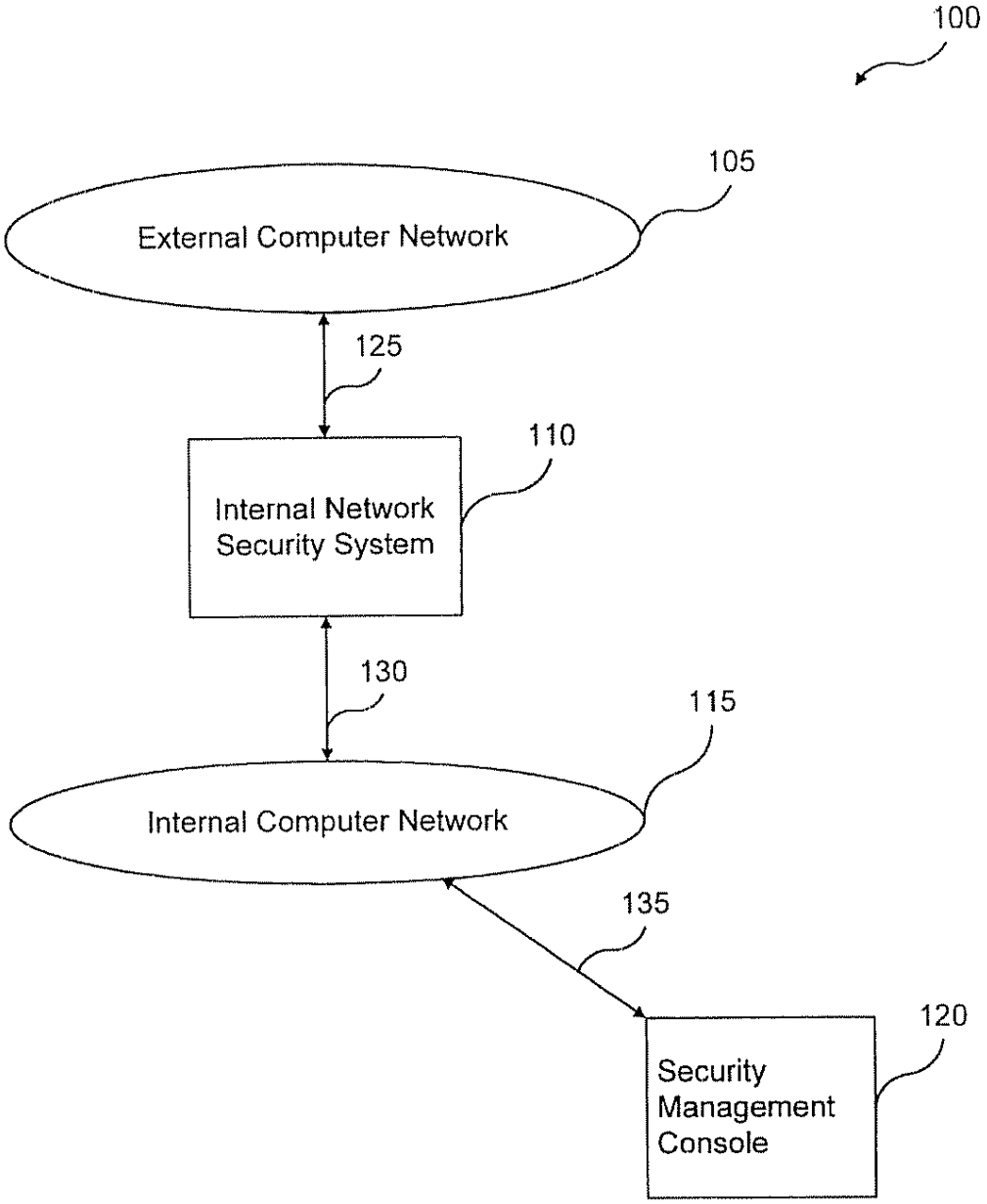


FIG. 1

www.freepatentsonline.com

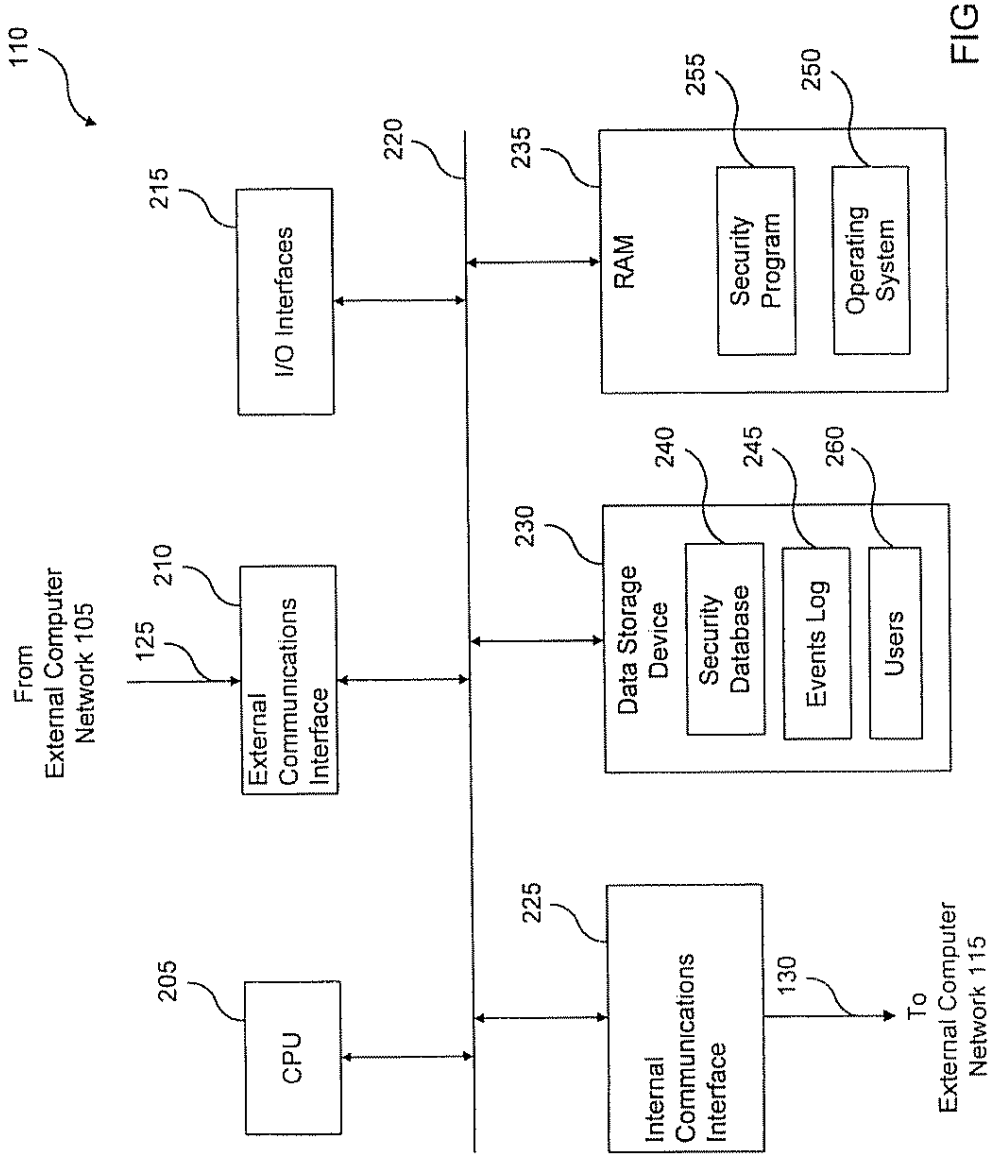


FIG. 2

www.freepatentsonline.com

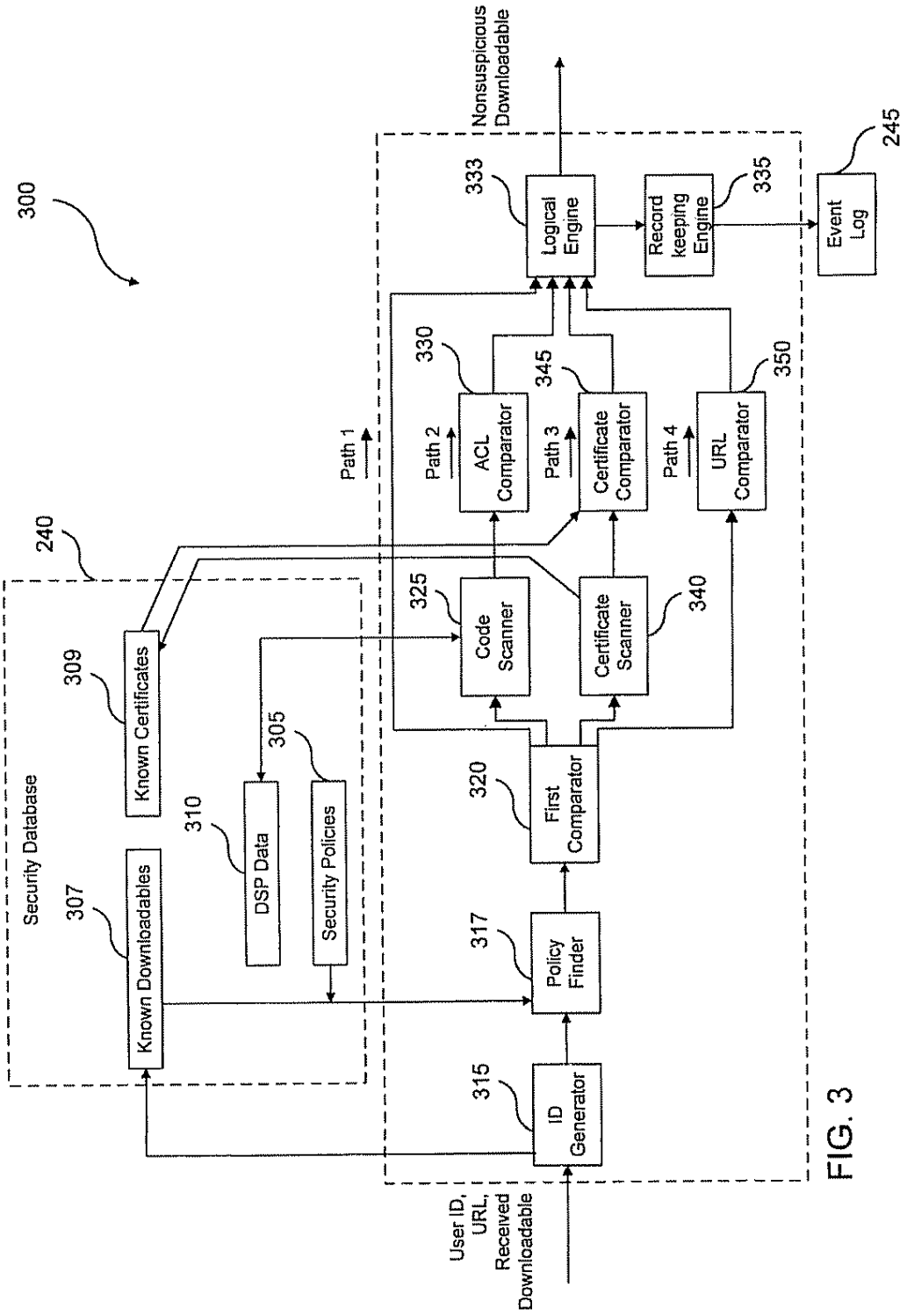


FIG. 3

www.freepatentsonline.com

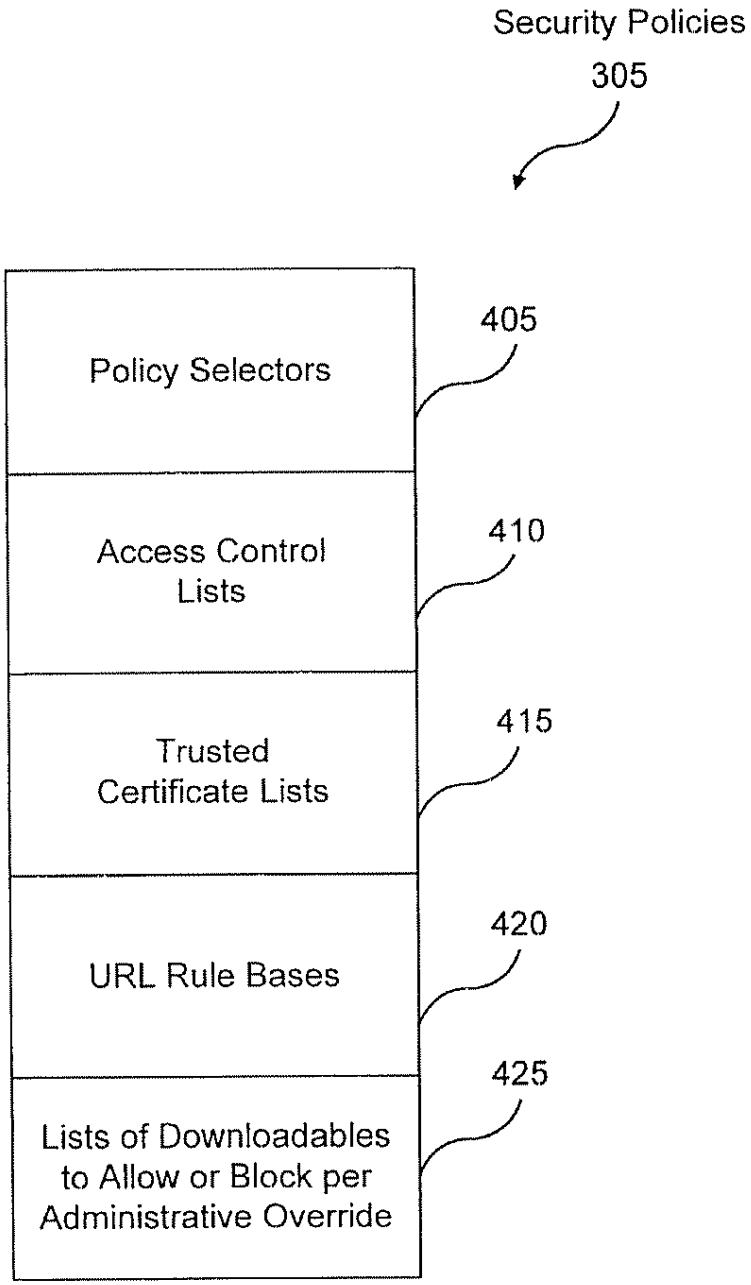


FIG. 4

www.freepatentsonline.com

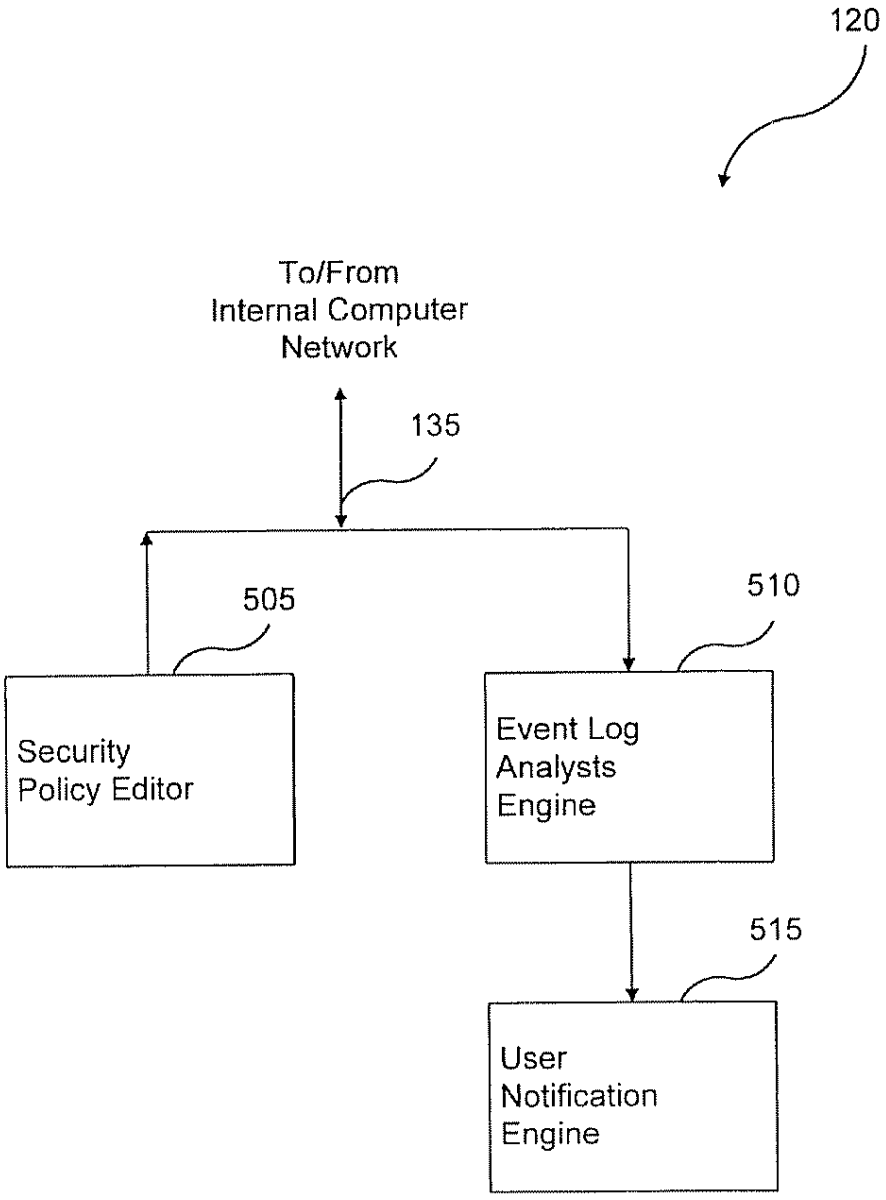


FIG. 5

www.freepatentsonline.com

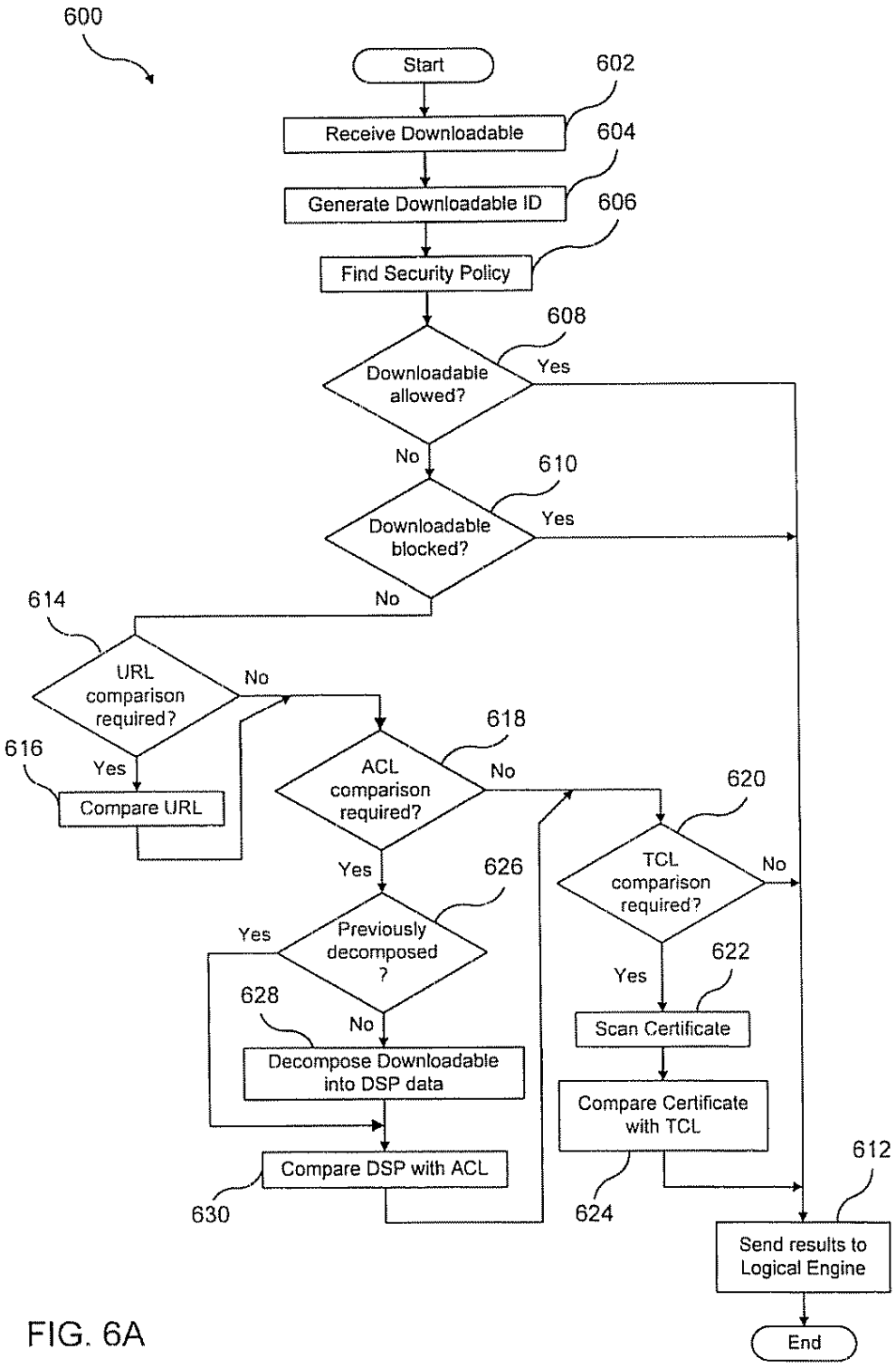


FIG. 6A

www.freepatentsonline.com

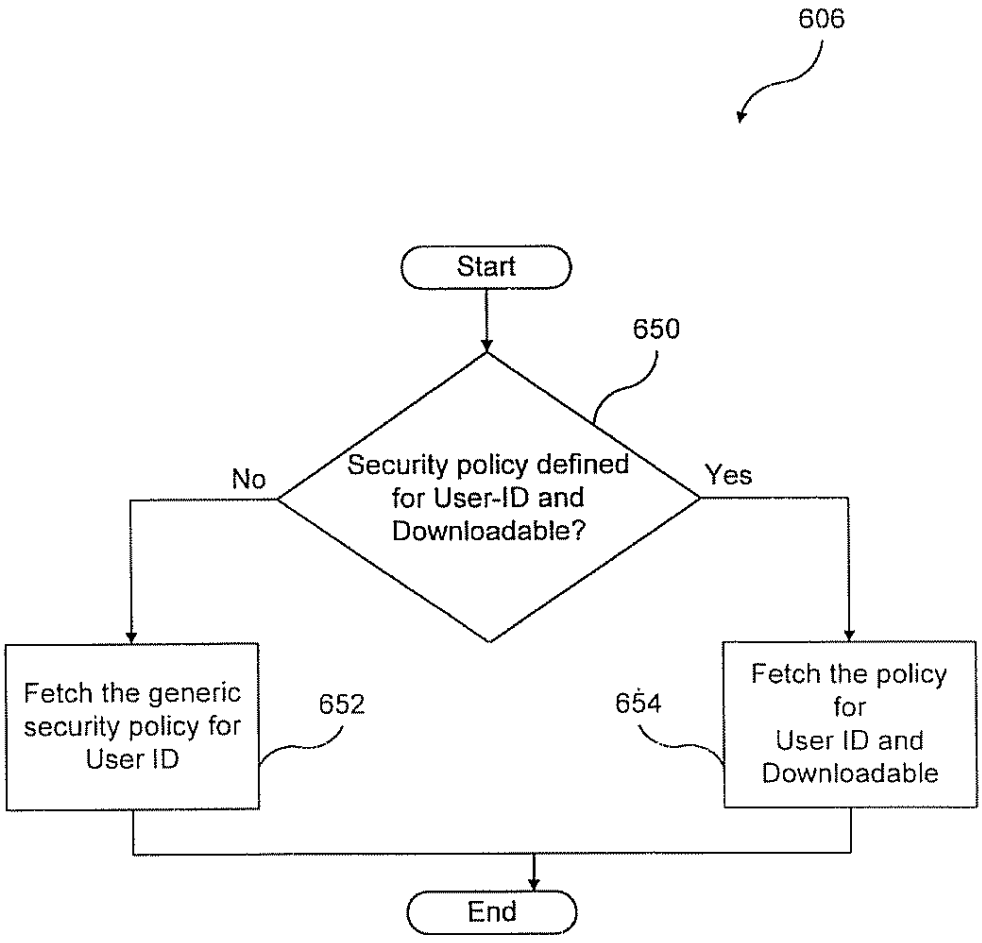


FIG. 6B

www.freepatentsonline.com

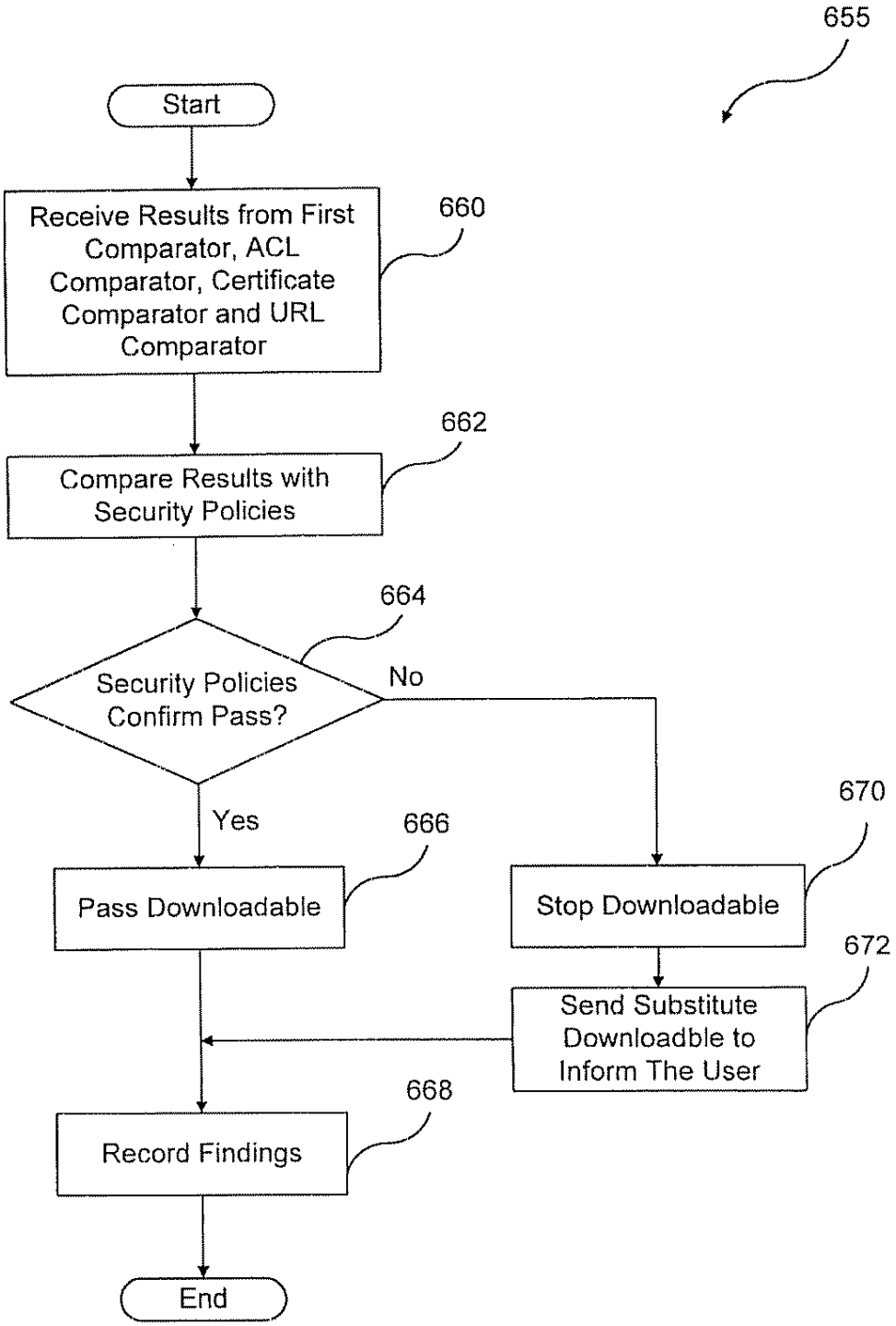


FIG. 6C

www.freepatentsonline.com

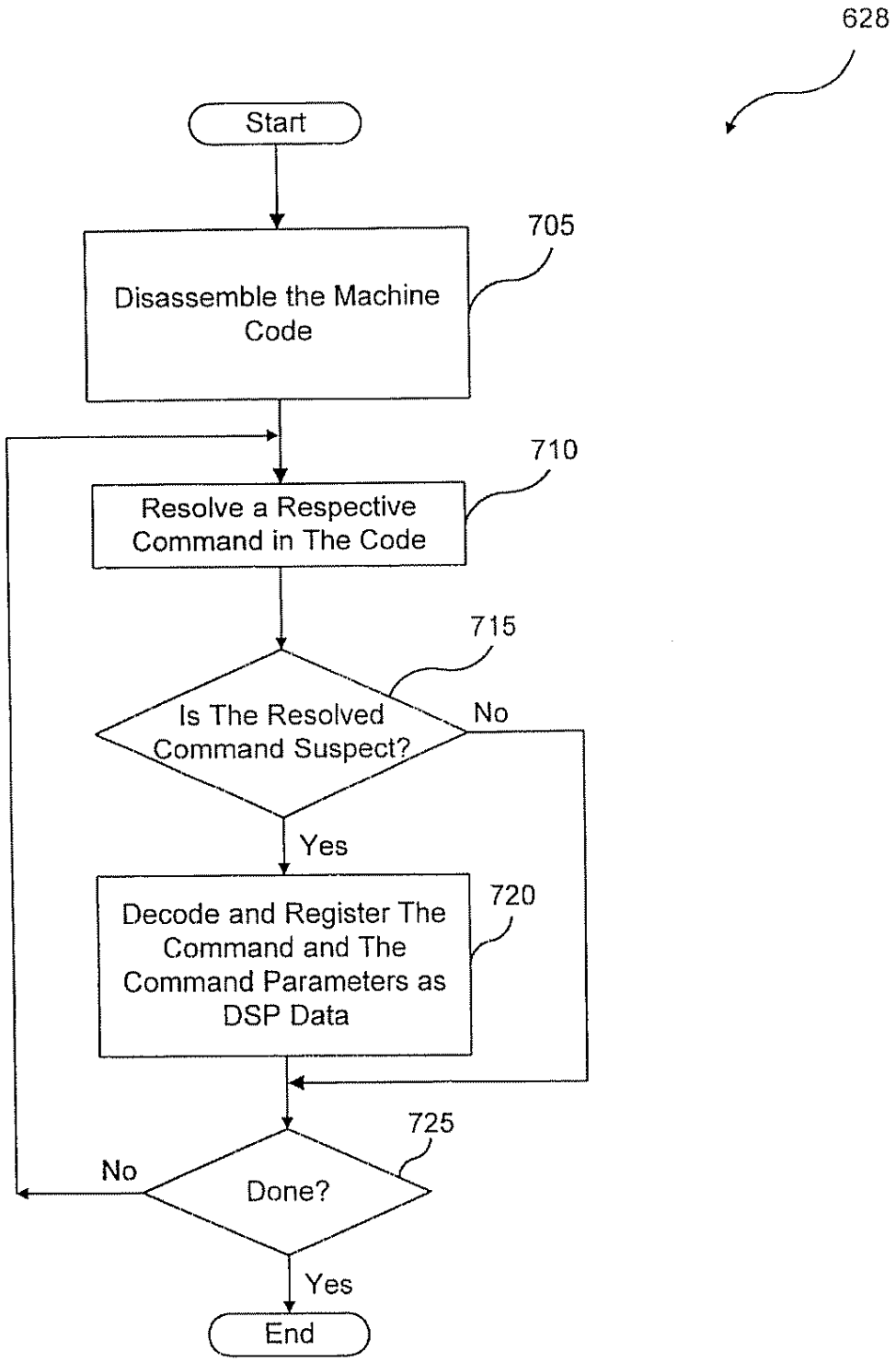


FIG. 7

www.freepatentsonline.com

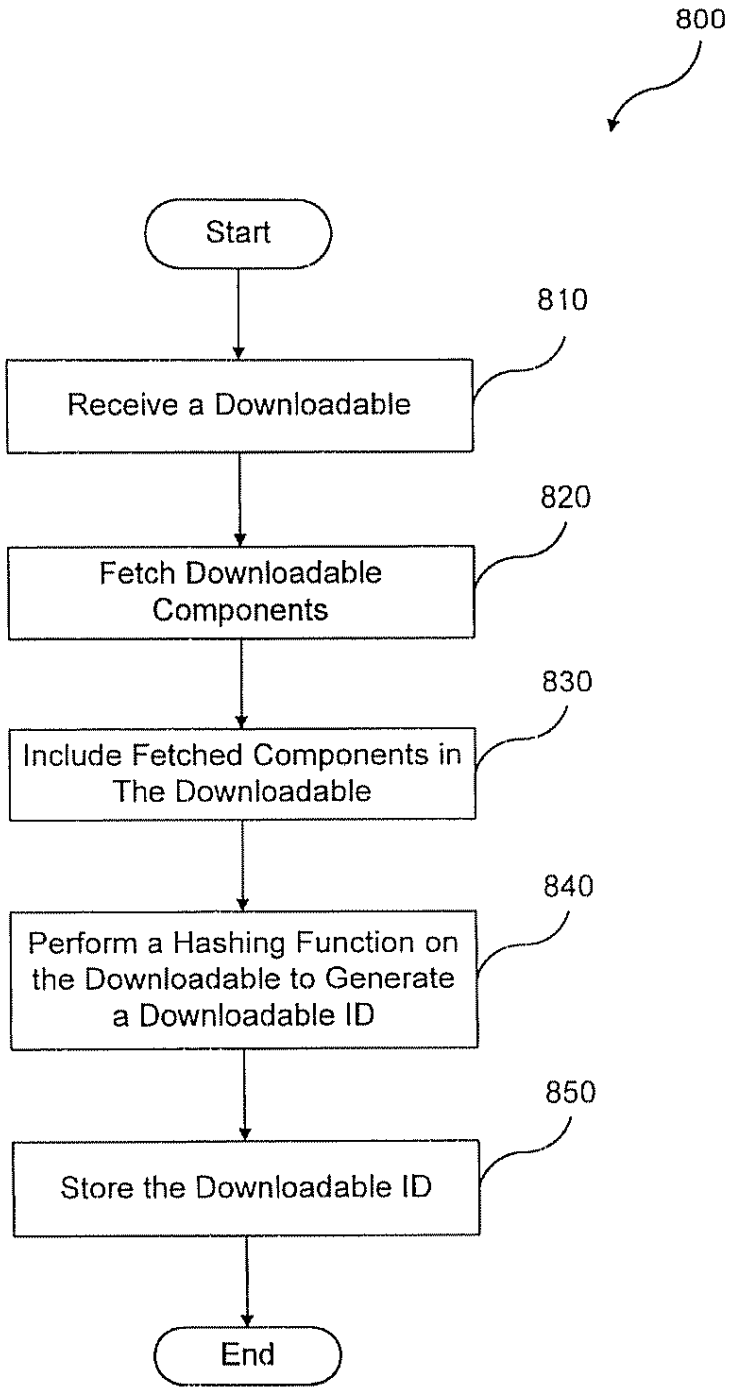


FIG. 8

www freepatentsonline.com

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

INCORPORATION BY REFERENCE TO RELATED APPLICATION

This application hereby incorporates by reference related U S patent application Ser No 08/790,097, entitled "System and Method for Protecting a Client from Hostile Downloadables," filed on Jan 29, 1997, by inventor Shlomo Touboul

PRIORITY REFERENCE TO PROVISIONAL APPLICATION

This application claims benefit of and hereby incorporates by reference provisional application Ser No 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov 8, 1996, by inventor Shlomo Touboul

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and method for protecting a computer and a network from hostile Downloadables

2. Description of the Background Art

The Internet is currently a collection of over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses"

Accordingly, programmers continue to design computer and computer network security systems for blocking these viruses from attacking both individual and network computers On the most part, these security systems have been relatively successful However, these security systems are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as "Downloadables" A Downloadable is an executable application program, which is downloaded from a source computer and run on the destination computer Downloadable is typically requested by an ongoing process such as by an Internet browser or web engine Examples of Downloadables include Java™ applets designed for use in the Java™ distributing environment developed by Sun Microsystems, Inc , JavaScript scripts also developed by Sun Microsystems, Inc , ActiveX™ controls designed for use in the ActiveX™ distributing environment developed by the Microsoft Corporation, and Visual Basic also developed by the Microsoft Corporation Therefore, a system and method are needed to protect a network from hostile Downloadables

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a network from suspicious Downloadables The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied based on the client/group and on the particular Downloadable received. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components

Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs Based on these tests, a logical engine can determine whether to allow or block the Downloadable

The present invention further provides a method for protecting a computer from suspicious Downloadables The method comprises the steps of receiving a Downloadable, comparing the Downloadable against a security policy to determine if the security policy has been violated, and discarding the Downloadable if the security policy has been violated

It will be appreciated that the system and method of the present invention may provide computer protection from known hostile Downloadables The system and method of the present invention may identify Downloadables that perform operations deemed suspicious The system and method of the present invention may examine the Downloadable code to determine whether the code contains any suspicious operations, and thus may allow or block the Downloadable accordingly

BRIEF DESCRIPTION OF THE DRAWINGS

FIG 1 is a block diagram illustrating a network system, in accordance with the present invention;

FIG 2 is a block diagram illustrating details of the internal network security system of FIG 1;

FIG 3 is a block diagram illustrating details of the security program and the security database of FIG 2;

FIG 4 is a block diagram illustrating details of the security policies of FIG 3;

FIG 5 is a block diagram illustrating details of the security management console of FIG 1;

FIG 6A is a flowchart illustrating a method of examining for suspicious Downloadables, in accordance with the present invention;

FIG 6B is a flowchart illustrating details of the step for finding the appropriate security policy of FIG 6A;

FIG 6C is a flowchart illustrating a method for determining whether an incoming Downloadable is to be deemed suspicious;

FIG 7 is a flowchart illustrating details of the FIG 6 step of decomposing a Downloadable; and

FIG 8 is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG 1 is a block diagram illustrating a network system **100**, in accordance with the present invention The network

www.freepatentsonline.com

system **100** includes an external computer network **105**, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a communications channel **125** to an internal network security system **110**. The network system **100** further includes an internal computer network **115**, such as a corporate Local Area Network (LAN), coupled via a communications channel **130** to the internal network computer system **110** and coupled via a communications channel **135** to a security management console **120**.

The internal network security system **110** examines Downloadables received from external computer network **105**, and prevents Downloadables deemed suspicious from reaching the internal computer network **115**. It will be further appreciated that a Downloadable is deemed suspicious if it performs or may perform any undesirable operation, or if it threatens or may threaten the integrity of an internal computer network **115** component. It is to be understood that the term "suspicious" includes hostile, potentially hostile, undesirable, potentially undesirable, etc. Security management console **120** enables viewing, modification and configuration of the internal network security system **110**.

FIG. **2** is a block diagram illustrating details of the internal network security system **110**, which includes a Central Processing Unit (CPU) **205**, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a signal bus **220**. The internal network security system **110** further includes an external communications interface **210** coupled between the communications channel **125** and the signal bus **220** for receiving Downloadables from external computer network **105**, and an internal communications interface **225** coupled between the signal bus **220** and the communications channel **130** for forwarding Downloadables not deemed suspicious to the internal computer network **115**. The external communications interface **210** and the internal communications interface **225** may be functional components of an integral communications interface (not shown) for both receiving Downloadables from the external computer network **105** and forwarding Downloadables to the internal computer network **115**.

Internal network security system **110** further includes Input/Output (I/O) interfaces **215** (such as a keyboard, mouse and Cathode Ray Tube (CRT) display), a data storage device **230** such as a magnetic disk, and a Random-Access Memory (RAM) **235**, each coupled to the signal bus **220**. The data storage device **230** stores a security database **240**, which includes security information for determining whether a received Downloadable is to be deemed suspicious. The data storage device **230** further stores a users list **260** identifying the users within the internal computer network **115** who may receive Downloadables, and an event log **245** which includes determination results for each Downloadable examined and runtime indications of the internal network security system **110**. An operating system **250** controls processing by CPU **205**, and is typically stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution. A security program **255** controls examination of incoming Downloadables, and also may be stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution by CPU **205**.

FIG. **3** is a block diagram illustrating details of the security program **255** and the security database **240**. The security program **255** includes an ID generator **315**, a policy finder **317** coupled to the ID generator **315**, and a first comparator **320** coupled to the policy finder **317**. The first comparator **320** is coupled to a logical engine **333** via four separate paths, namely, via Path 1, via Path 2, via Path 3 and via Path 4. Path 1 includes a direct connection from the first comparator **320** to the logical engine **333**. Path 2 includes a code scanner coupled to the first comparator **320**, and an Access Control List (ACL) comparator **330** coupling the code scanner **325** to the logical engine **333**. Path 3 includes a certificate scanner **340** coupled to the first comparator **320**, and a certificate comparator **345** coupling the certificate scanner **340** to the logical engine **333**. Path 4 includes a Uniform Resource Locator (URL) comparator **350** coupling the first comparator **320** to the logical engine **3330**. A record-keeping engine **335** is coupled between the logical engine **333** and the event log **245**.

The security program **255** operates in conjunction with the security database **240**, which includes security policies **305**, known Downloadables **307**, known Certificates **309** and Downloadable Security Profile (DSP) data **310** corresponding to the known Downloadables **307**. Security policies **305** includes policies specific to particular users **260** and default (or generic) policies for determining whether to allow or block an incoming Downloadable. These security policies **305** may identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable. Referring to FIG. **4**, security policies **305** include policy selectors **405**, access control lists **410**, trusted certificate lists **415**, URL rule bases **420**, and lists **425** of Downloadables to allow or to block per administrative override.

Known Downloadables **307** include lists of Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, of Downloadables which OEMs know to be non-hostile, and of Downloadables previously received by this security program **255**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by each known Downloadable **307**, and may also include the respective arguments of these operations. An identified argument of an operation is referred to as "resolved." An unidentified argument is referred to as "unresolved." DSP data **310** is described below with reference to the code scanner **325**.

The ID generator **315** receives a Downloadable (including the URL from which it came and the userID of the intended recipient) from the external computer network **105** via the external communications interface **210**, and generates a Downloadable ID for identifying each Downloadable. The Downloadable ID preferably includes a digital hash of the complete Downloadable code. The ID generator **315** preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator **315** may prefetch all classes embodied in or identified by the Java™ applet bytecode to generate the Downloadable ID. Similarly, the ID generator **315** may retrieve all components listed in the INF file for an ActiveX™ control to compute a Downloadable ID. Accordingly, the Downloadable ID for the Downloadable will be the same each time the ID generator **315** receives the same Downloadable. The ID generator **315** adds the generated Downloadable ID to the list of known Downloadables **307** (if it is not already listed). The ID generator **315** then forwards the Downloadable and Downloadable ID to the policy finder **317**.

The policy finder **317** uses the userID of the intended user and the Downloadable ID to select the specific security policy **305** that shall be applied on the received Downloadable. If there is a specific policy **305** that was defined for the user (or for one of its super groups) and the Downloadable, then the policy is selected. Otherwise the generic policy **305**

www.freepatentsonline.com

that was defined for the user (or for one of its super groups) is selected. The policy finder **317** then sends the policy to the first comparator **320**.

The first comparator **320** receives the Downloadable, the Downloadable ID and the security policy **305** from the policy finder **317**. The first comparator **320** examines the security policy **305** to determine which steps are needed for allowing the Downloadable. For example, the security policy **305** may indicate that, in order to allow this Downloadable, it must pass all four paths, Path 1, Path 2, Path 3 and Path 4. Alternatively, the security policy **305** may indicate that to allow the Downloadable, it must pass only one of the paths. The first comparator **320** responds by forwarding the proper information to the paths identified by the security policy **305**.

Path 1

In path 1, the first comparator **320** checks the policy selector **405** of the security policy **305** that was received from the policy finder **317**. If the policy selector **405** is either "Allowed" or "Blocked," then the first comparator **320** forwards this result directly to the logical engine **333**. Otherwise, the first comparator **320** invokes the comparisons in path 2 and/or path 3 and/or path 4 based on the contents of policy selector **405**. It will be appreciated that the first comparator **320** itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override **425**. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked."

Alternatively, the logical engine **333** may receive the results of each of the paths and based on the policy selector **405** may institute the final determination whether to allow or block the Downloadable. The first comparator **320** informs the logical engine **333** of the results of its comparison.

Path 2

In path 2, the first comparator **320** delivers the Downloadable, the Downloadable ID and the security policy **305** to the code scanner **325**. If the DSP data **310** of the received Downloadable is known, the code scanner **325** retrieves and forwards the information to the ACL comparator **330**. Otherwise, the code scanner **325** resolves the DSP data **310**. That is, the code scanner **325** uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data **310**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable **307**, and may also include the respective arguments of these operations. For example, DSP data **310** may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner **325** may generate the DSP data **310** as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner **325** may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker.

An Example List of Operations Deemed Potentially Hostile

File operations: READ a file, WRITE a file;

Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET;

Registry operations: READ a registry item, WRITE a registry item;

Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAD, KILL PROCESS/THREAD, CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc; and

Resource usage thresholds: memory, CPU, graphics, etc

In the preferred embodiment, the code scanner **325** performs a full-content inspection. However, for improved speed but reduced security, the code scanner **325** may examine only a portion of the Downloadable such as the Downloadable header. The code scanner **325** then stores the DSP data into DSP data **310** (corresponding to its Downloadable ID), and sends the Downloadable, the DSP data to the ACL comparator **330** for comparison with the security policy **305**.

The ACL comparator **330** receives the Downloadable, the corresponding DSP data and the security policy **305** from the code scanner **325**, and compares the DSP data against the security policy **305**. That is, the ACL comparator **330** compares the DSP data of the received Downloadable against the access control lists **410** in the received security policy **305**. The access control list **410** contains criteria indicating whether to pass or fail the Downloadable. For example, an access control list may indicate that the Downloadable fails if the DSP data includes a WRITE command to a system file. The ACL comparator **330** sends its results to the logical engine **333**.

Path 3

In path 3, the certificate scanner **340** determines whether the received Downloadable was signed by a certificate authority, such as VeriSign, Inc., and scans for a certificate embodied in the Downloadable. The certificate scanner **340** forwards the found certificate to the certificate comparator **345**. The certificate comparator **345** retrieves known certificates **309** that were deemed trustworthy by the security administrator and compares the found certificate with the known certificates **309** to determine whether the Downloadable was signed by a trusted certificate. The certificate comparator **345** sends the results to the logical engine **333**.

Path 4

In path 4, the URL comparator **350** examines the URL identifying the source of the Downloadable against URLs stored in the URL rule base **420** to determine whether the Downloadable comes from a trusted source. Based on the security policy **305**, the URL comparator **350** may deem the Downloadable suspicious if the Downloadable comes from an untrustworthy source or if the Downloadable did not come from a trusted source. For example, if the Downloadable comes from a known hacker, then the Downloadable may be deemed suspicious and presumed hostile. The URL comparator **350** sends its results to the logical engine **333**.

The logical engine **333** examines the results of each of the paths and the policy selector **405** in the security policy **305** to determine whether to allow or block the Downloadable. The policy selector **405** includes a logical expression of the results received from each of the paths. For example, the logical engine **333** may block a Downloadable if it fails any one of the paths, i.e., if the Downloadable is known hostile (Path 1), if the Downloadable may request suspicious operations (Path 2), if the Downloadable was not signed by a trusted certificate authority (Path 3), or if the Downloadable came from an untrustworthy source (Path 4). The logical engine **333** may apply other logical expressions according to the policy selector **405** embodied in the security policy **305**. If the policy selector **405** indicates that the Downloadable may pass, then the logical engine **333** passes the Downloadable to its intended recipient. Otherwise, if the policy selector **405** indicates that the Downloadable should be blocked, then the logical engine **333** forwards a non-hostile Downloadable to the intended recipient to inform the user

www.freepatentsonline.com

that internal network security system **110** discarded the original Downloadable Further, the logical engine **333** forwards a status report to the record-keeping engine **335**, which stores the reports in event log **245** in the data storage device **230** for subsequent review, for example, by the MIS director

FIG. **5** is a block diagram illustrating details of the security management console **120**, which includes a security policy editor **505** coupled to the communications channel **135**, an event log analysis engine **510** coupled between communications channel **135** and a user notification engine **515**, and a Downloadable database review engine **520** coupled to the communications channel **135** The security management console **120** further includes computer components similar to the computer components illustrated in FIG. **2**.

The security policy editor **505** uses an I/O interface similar to I/O interface **215** for enabling authorized user modification of the security policies **305**. That is, the security policy editor **505** enables the authorized user to modify specific security policies **305** corresponding to the users **260**, the default or generic security policy **305**, the Downloadables to block per administrative override, the Downloadables to allow per administrative override, the trusted certificate lists **415**, the policy selectors **405**, the access control lists **410**, the URLs in the URL rule bases **420**, etc. For example, if the authorized user learns of a new hostile Downloadable, then the user can add the Downloadable to the Downloadables to block per system override.

The event log analysis engine **510** examines the status reports contained in the event log **245** stored in the data storage device **230**. The event log analysis engine **510** determines whether notification of the user (e g , the security system manager or MIS director) is warranted. For example, the event log analysis engine **510** may warrant user notification whenever ten (10) suspicious Downloadables have been discarded by internal network security system **110** within a thirty (30) minute period, thereby flagging a potential imminent security threat. Accordingly, the event log analysis engine **510** instructs the user notification engine **515** to inform the user. The user notification engine **515** may send an e-mail via internal communications interface **220** or via external communications interface **210** to the user, or may display a message on the user's display device (not shown).

FIG. **6A** is a flowchart illustrating a method **600** for protecting an internal computer network **115** from suspicious Downloadables. Method **600** begins with the ID generator **315** in step **602** receiving a Downloadable The ID generator **315** in step **604** generates a Downloadable ID identifying the received Downloadable, preferably, by generating a digital hash of the Downloadable code (including prefetched components) The policy finder **317** in step **606** finds the appropriate security policy **305** corresponding to the userID specifying intended recipient (or the group to which the intended recipient belongs) and the Downloadable. The selected security policy **305** may be the default security policy **305** Step **606** is described in greater detail below with reference to FIG. **6B**.

The first comparator **320** in step **608** examines the lists of Downloadables to allow or to block per administrative override **425** against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically If so, then in step **612** the first comparator **320** sends the results to the logical engine **333** If not, then the method **600** proceeds to step **610**. In step **610**, the first comparator **620** examines the lists of Downloadables to block per administrative override **425** against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically If so, then the first comparator **420** in step **612** sends the results to the logical engine **333** Otherwise, method **600** proceeds to step **614**

In step **614**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 4 If not, then method **600** jumps to step **618**. If so, then the URL comparator **350** in step **616** compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases **420**, and then method **600** proceeds to step **618**

In step **618**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 2 If not, then method **600** jumps to step **620**. Otherwise, the code scanner **235** in step **626** examines the DSP data **310** based on the Downloadable ID of the incoming Downloadable to determine whether the Downloadable has been previously decomposed If so, then method **600** jumps to step **630**. Otherwise, the code scanner **325** in step **628** decomposes the Downloadable into DSP data. Downloadable decomposition is described in greater detail with reference to FIG **7** In step **630**, the ACL comparator **330** compares the DSP data of the incoming Downloadable against the access control lists **410** (which include the criteria necessary for the Downloadable to fail or pass the test)

In step **620**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 3 If not, then method **600** returns to step **612** to send the results of each of the test performed to the logical engine **333**. Otherwise, the certificate scanner **622** in step **622** scans the Downloadable for an embodied certificate The certificate comparator **345** in step **624** retrieves trusted certificates from the trusted certificate lists (TCL) **415** and compares the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source. Method **600** then proceeds to step **612** by the certificate scanner **345** sending the results of each of the paths taken to the logical engine **333**. The operations of the logical engine **333** are described in greater detail below with reference to FIG **6C**. Method **600** then ends

One skilled in the art will recognize that the tests may be performed in a different order, and that each of the tests need not be performed Further, one skilled in the art will recognize that, although path 1 is described in FIG. **6A** as an automatic allowance or blocking, the results of Path 1 may be another predicate to be applied by the logical engine **333**. Further, although the tests are shown serially in FIG. **6A**, the tests may be performed in parallel as illustrated in FIG. **3**

FIG. **6B** is a flowchart illustrating details of step **606** of FIG. **6A** (referred to herein as method **606**). Method **606** begins with the policy finder **317** in step **650** determining whether security policies **305** include a specific security policy corresponding to the userID and the Downloadable If so, then the policy finder **317** in step **654** fetches the corresponding specific policy **305** If not, then the policy finder **317** in step **652** fetches the default or generic security policy **305** corresponding to the userID. Method **606** then ends.

FIG **6C** is a flowchart illustrating details of a method **655** for determining whether to allow or to block the incoming Downloadable. Method **655** begins with the logical engine **333** in step **660** receiving the results from the first comparator **320**, from the ACL comparator **330**, from the certificate

www.freepatentsonline.com

comparator **345** and from the URL comparator **350**. The logical engine **333** in step **662** compares the results with the policy selector **405** embodied in the security policy **305**, and in step **664** determines whether the policy selector **405** confirms the pass. For example, the policy selector **405** may indicate that the logical engine **333** pass the Downloadable if it passes one of the tests of Path 1, Path 2, Path 3 and Path 4. If the policy selector **405** indicates that the Downloadable should pass, then the logical engine **333** in step **666** passes the Downloadable to the intended recipient. In step **668**, the logical engine **333** sends the results to the record-keeping engine **335**, which in turn stores the results in the event log **245** for future review. Method **655** then ends. Otherwise, if the policy selector **405** in step **664** indicates that the Downloadable should not pass, then the logical engine **333** in step **670** stops the Downloadable and in step **672** sends a non-hostile substitute Downloadable to inform the user that the incoming Downloadable has been blocked. Method **655** then jumps to step **668**.

FIG. **7** is a flowchart illustrating details of step **628** of FIG. **6**A (referred to herein as method **628**) for decomposing a Downloadable into DSP data **310**. Method **628** begins in step **705** with the code scanner **325** disassembling the machine code of the Downloadable. The code scanner **325** in step **710** resolves a respective command in the machine code, and in step **715** determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. **3**). If not, then the code scanner **325** in step **725** determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method **628** ends. Otherwise, method **628** returns to step **710**.

Otherwise, if the code scanner **325** in step **715** determines that the resolved command is suspect, then the code scanner **325** in step **720** decodes and registers the suspicious command and its command parameters as DSP data **310**. The code scanner **325** in step **720** registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method **628** then jumps to step **725**.

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable. Method **800** begins with the ID generator **315** in step **810** receiving a Downloadable from the external computer network **105**. The ID generator **315** in step **820** may fetch some or all components referenced in the Downloadable code, and in step **830** includes the fetched components in the Downloadable code. The ID generator **315** in step **840** performs a hashing function on at least a portion of the Downloadable code to generate a Downloadable ID. The ID generator **315** in step **850** stores the generated Downloadable ID in the security database **240** as a reference to the DSP data **310**. Accordingly, the Downloadable ID will be the same for the identical Downloadable each time it is encountered.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method, comprising the steps of:

receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client;

comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and

preventing execution of the Downloadable by the client if the security policy has been violated.

2. The method of claim **1**, further comprising the step of decomposing the Downloadable into the Downloadable security profile data.

3. The method of claim **2**, wherein the security policy includes an access control list and further comprising the step of comparing the Downloadable security profile data against the access control list.

4. The method of claim **1**, further comprising the steps of scanning for a certificate and comparing the certificate against a trusted certificate.

5. The method of claim **1**, further comprising the step of comparing the URL from which the Downloadable originated against a known URL.

6. The method of claim **5**, wherein the known URL is a trusted URL.

7. The method of claim **5**, wherein the known URL is an untrusted URL.

8. The method of claim **1**, wherein the Downloadable includes a Java™ applet.

9. The method of claim **1**, wherein the Downloadable includes an ActiveX™ control.

10. The method of claim **1**, wherein the Downloadable includes a JavaScript™ script.

11. The method of claim **1**, wherein the Downloadable includes a Visual Basic script.

12. The method of claim **1**, wherein

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

13. The method of claim **1**, wherein

the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

14. The method of claim **1**, wherein

the client belongs to a particular group; and

the security policy includes a specific security policy corresponding to the particular group.

15. The method of claim **1**, further comprising, after preventing execution of the Downloadable, the step of sending a substitute non-hostile Downloadable to the client for informing the client.

16. The method of claim **1**, further comprising, after preventing execution of the Downloadable, the step of recording the violation in an event log.

17. The method of claim **1**, further comprising the step of computing a Downloadable ID to identify the Downloadable.

18. The method of claim **16**, further comprising the steps of fetching components identified by the Downloadable and including the fetched components in the Downloadable.

www.freepatentsonline.com

19 The method of claim 18, further comprising the step of performing a hashing function on the Downloadable to compute a Downloadable ID to identify the Downloadable.

20 The method of claim 18, further comprising the step of fetching all components identified by the Downloadable.

21 The method of claim 1 further comprising the step of examining the intended recipient userID to determine the appropriate security policy.

22 The method of claim 20, wherein the appropriate security policy includes a default security policy.

23 The method of claim 1, further comprising the step of examining the Downloadable to determine the appropriate security policy.

24 The method of claim 1, further comprising the step of comparing the Downloadable against a known Downloadable.

25 The method of claim 24, wherein the known Downloadable is hostile.

26 The method of claim 24, wherein the known Downloadable is non-hostile.

27 The method of claim 24, further comprising the step of including a previously received Downloadable as a known Downloadable.

28 The method of claim 27, wherein the security policy identifies a Downloadable to be blocked per administrative override.

29 The method of claim 28, wherein the security policy identifies a Downloadable to be allowed per administrative override.

30 The method of claim 1, further comprising the step of informing a user upon detection of a security policy violation.

31 The method of claim 1, further comprising the steps of recognizing the incoming Downloadable, and obtaining the Downloadable security profile data for the incoming Downloadable from memory.

32 A system for execution by a server that serves as a gateway to a client, the system comprising:

a security policy;

an interface for receiving an incoming Downloadable addressed to a client;

a comparator, coupled to the interface, for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against the security policy to determine if the security policy has been violated; and

a logical engine for preventing execution of the Downloadable by the client if the security policy has been violated.

33 The system of claim 32, wherein the Downloadable includes a Java™ applet.

34 The system of claim 32, wherein the Downloadable includes ActiveX™ control.

35 The system of claim 32, wherein the Downloadable includes a JavaScript™ script.

36 The system of claim 32, wherein the Downloadable includes a Visual Basic script.

37 The system of claim 32, wherein

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

38 The system of claim 32, wherein

the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

39 The system of claim 32, wherein

the client belongs to a particular group; and

the security policy includes a specific security policy corresponding to the particular group.

40 The system of claim 32, further comprising an ID generator coupled to the interface for computing a Downloadable ID identifying the Downloadable.

41 The system of claim 40, wherein the ID generator prefetches all components of the Downloadable and uses all components to compute the Downloadable ID.

42 The system of claim 41, wherein the ID generator computes the digital hash of all the prefetched components.

43 The system of claim 32, further comprising a policy finder for finding the security policy.

44 The system of claim 43, wherein the policy finder finds the security policy based on the user.

45 The system of claim 43 wherein the policy finder finds the security policy based on the user and the Downloadable.

46 The system of claim 43, wherein the policy finder obtains the default security policy.

47 The system of claim 32 wherein the comparator examines the security policy to determine which tests to apply.

48 The system of claim 47 wherein the comparator compares the Downloadable against a known Downloadable.

49 The system of claim 48, wherein the known Downloadable is hostile.

50 The system of claim 48, wherein the known Downloadable is non-hostile.

51 The system of claim 32, wherein the security policy identifies a Downloadable to be blocked per administrative override.

52 The system of claim 32, wherein the security policy identifies a Downloadable to be allowed per administrative override.

53 The system of claim 32, wherein

the comparator sends a substitute non-hostile Downloadable to the client for informing the client.

54 The system of claim 32, further comprising a code scanner coupled to the comparator for decomposing the Downloadable into the Downloadable security profile data.

55 The system of claim 54, further comprising an ACL comparator coupled to the code scanner for comparing the Downloadable security profile data against an access control list.

56 The system of claim 32, further comprising a certificate scanner coupled to the comparator for examining the Downloadable for a certificate.

57 The system of claim 56, further comprising a certificate comparator coupled to the certificate scanner for comparing the certificate against a trusted certificate.

58 The system of claim 32, further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL.

59 The system of claim 58, wherein the known URL identifies an untrusted URL.

60 The system of claim 58, wherein the known URL identifies a trusted URL.

61 The system of claim 31, wherein the logical engine responds according to the security policy.

62 The system of claim 31, further comprising a record-keeping engine coupled to the comparator for recording results in an event log.

63 The system of claim 32, further comprising memory storing the Downloadable security profile data for the incoming Downloadable.

www.freepatentsonline.com

64. A system for execution on a server that serves as a gateway to a client, comprising:

means for receiving an incoming Downloadable addressed to a client;

means for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and

means for preventing execution of the Downloadable by the client if the security policy has been violated

65. A computer-readable storage medium storing program code for causing a server that serves as a gateway to a client to perform the steps of:

receiving an incoming Downloadable addressed to a client;

comparing Downloadable security profile data pertaining to the Downloadable against a security policy to determine if the security policy has been violated; and

preventing execution of the Downloadable by the client if the security policy has been violated

66. A method, comprising:

receiving a Downloadable;

decomposing the Downloadable into Downloadable security profile data; the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable,

comparing the Downloadable security profile data against a security policy; and

preventing execution of the Downloadable if the Downloadable security profile data violates the security policy.

67. The method of claim 66, further comprising:

fetching all components referenced by the Downloadable;

performing a hashing function of the Downloadable and the components fetched to compute a Downloadable ID; and

storing the Downloadable security profile data and the Downloadable ID in memory

68. A method, comprising:

providing memory storing known-Downloadable security profile data and a that includes a list a suspicious computer operations that may be attempted by a Downloadable known-Downloadable ID corresponding to the Downloadable security profile data;

receiving an incoming Downloadable;

fetching all components referenced by the incoming Downloadable;

performing a hashing function of the Downloadable and the components to compute an incoming-Downloadable ID;

comparing the known-Downloadable ID against the incoming-Downloadable ID;

retrieving the Downloadable security profile data if the known-Downloadable ID and the incoming-Downloadable ID match; and

comparing the Downloadable security profile data against a security policy to determine if the incoming Downloadable violates the security policy.

* * * * *

www.freepatentsonline.com

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,092,194
DATED : July 18, 2000
INVENTOR(S) : Shlomo Touboul

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 13,
Line 19, after "to the Downloadable" and before "against a security" insert --, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, --

Column 14,
Line 12, after "profile data and" and before "that includes" delete -- a --

Signed and Sealed this

Fifth Day of February, 2002

Attest:

Attesting Officer

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

www.freepatentsonline.com

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israeli corporation,	)	
Plaintiff,	)	C.A. No. 06-00369 GMS
v.	)	DEMAND FOR JURY TRIAL
SECURE COMPUTING CORPORATION, a Delaware corporation; CYBERGUARD CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100,	)	
Defendants.	)	

ANSWER AND COUNTERCLAIMS OF DEFENDANTS SECURE COMPUTING CORPORATION, CYBERGUARD CORPORATION, AND WEBWASHER AG

Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG (collectively referred to as "Secure Computing") for their Answer to Plaintiff's Complaint, states as follows:

GENERAL DENIAL

Secure Computing denies each and every allegation, matter or thing contained in the Complaint which is not expressly admitted, qualified or answered herein.

THE PARTIES

1. Secure Computing lacks sufficient knowledge to form a belief as to the truth or falsity of the allegations contained in paragraph 1 of the Complaint and therefore denies the same.

2. Secure Computing admits the allegations of paragraph 2 of the Complaint.

3. Secure Computing denies the allegations of paragraph 3 of the Complaint.

4. Secure Computing denies that Defendant Webwasher AG has a branch office in the United States. Secure Computing denies that Defendant Webwasher AG is a wholly-owned subsidiary of CyberGuard Corporation. Secure Computing admits that Webwasher AG is a corporation organized and existing under the laws of Germany and a subsidiary of Secure Computing Corporation.

JURISDICTION AND VENUE

5. The allegations in paragraph 5 are legal conclusions and do not require a responsive pleading. To the extent a response is required, Secure Computing does not dispute that jurisdiction is proper under 28 U.S.C. §§ 1331 and 1338.

6. The allegations in paragraph 6 are legal conclusions and do not require a responsive pleading. To the extent a response is required, Secure Computing does not dispute that venue is proper under 28 U.S.C. §§ 1391(b) and (c) and/or under 28 U.S.C. § 1400(b) and that personal jurisdiction is proper over Defendants. Secure Computing denies that Defendants CyberGuard Corp. and Webwasher AG are Delaware corporations. Secure Computing denies that any of the Defendants have and continue to infringe, contributorily infringe and/or induce infringement of U.S. Patent No. 6,092,194.

PLAINTIFF'S PATENT

7. Secure Computing admits that Exhibit A to the Complaint is a copy of the '194 patent. Secure Computing denies any and all other allegations of paragraph 7 of the Complaint.

8. Secure Computing denies the allegations of paragraph 8 of the Complaint.

PATENT INFRINGEMENT

9. Secure Computing Corporation admits that it is in the business of developing and distributing network and systems security solutions to organizations. Secure Computing denies any and all other allegations of paragraph 9 of the Complaint.

10. Secure Computing admits that Defendant CyberGuard was in the business of developing and distributing information security solutions, but denies that CyberGuard is currently engaging in business. Secure Computing denies any and all other allegations of paragraph 10 of the Complaint.

11. Secure Computing admits that Defendant Webwasher AG is in the business of developing and distributing Internet and email content security and filtering solutions. Secure Computing denies any and all other allegations of paragraph 11 of the Complaint.

FIRST CAUSE OF ACTION

(Infringement of the '194 Patent)

12. Secure Computing admits that in paragraph 12 of the Complaint Plaintiff re-alleges the allegations set forth in paragraphs 1 through 11 in the Complaint and in response to paragraph 12 of the Complaint, Secure Computing restates and incorporates by reference its answers to paragraphs 1 through 11 and denies any allegation not expressly admitted.

13. Secure Computing denies the allegations of paragraph 13 of the Complaint.

14. Secure Computing denies the allegations of paragraph 14 of the Complaint.

15. Secure Computing denies the allegations of Plaintiff's second paragraph 14 (which appears to have been numbered in error) of the Complaint.

AFFIRMATIVE DEFENSES

FIRST AFFIRMATIVE DEFENSE

16. Plaintiff fails to state a claim upon which relief can be granted.

SECOND AFFIRMATIVE DEFENSE

17. Plaintiff's claims are barred by the doctrines of waiver, estoppel, and laches.

THIRD AFFIRMATIVE DEFENSE

18. Plaintiff's asserted patent, United States Patent No. 6,092,194 ("the '194 patent"), is invalid, unenforceable, and/or void for failure to satisfy the requirements of patentability contained in 35 U.S.C. Section 101, et seq., including, but not limited to, Sections 102, 103, and for lack of enablement and inadequate written description under 35 U.S.C. section 112, and for failure to disclose best mode.

19. Secure Computing reserves its right to assert additional grounds for the invalidity or unenforceability of the '194 patent if it discovers such grounds during the course of the litigation.

FOURTH AFFIRMATIVE DEFENSE

20. Secure Computing does not infringe, has not induced infringement, and has not contributed to infringement of any valid and enforceable claim of any patent owned by Plaintiff.

FIFTH AFFIRMATIVE DEFENSE

21. Plaintiff's request for damages arising from alleged infringement, whether direct or otherwise, is barred by Plaintiff's failure to plead marking, failure to mark and/or failure to require licensees to mark.

COUNTERCLAIMS

22. Defendants Secure Computing Corporation and Webwasher AG (collectively referred to as "Secure Computing"), for their Counterclaims against Plaintiff, state:

COUNTERCLAIM FOR DECLARATORY JUDGMENT OF INVALIDITY, UNENFORCEABILITY, AND NONINFRINGEMENT

23. Defendant Secure Computing Corporation is corporation organized and existing under the laws of the State of Delaware, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124. Defendant Webwasher AG is a corporation organized and existing under the laws of Germany and a subsidiary of Secure Computing Corporation.

24. On information and belief, Plaintiff Finjan Software Ltd. is a corporation organized and existing under the laws of Israel, with its principal place of business at Hamachsheve St. 1, New Industrial Area, Netanya, 42504, Israel.

25. This is an action for a declaratory judgment, together with such relief based thereon as may be necessary or proper, pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. Sections 2201, 2202. There is an actual controversy between Plaintiff and Secure Computing arising under the United States patent laws, Title 35 of the United States Code.

26. This Counterclaim arises under the Patent Laws of the United States, Title 35, United States Code. The jurisdiction of this Court is founded upon and arises under Title 28, United States Code sections 1338(a), and under the Federal Declaratory Judgment Act, Title 28, sections 2201 and 2202. Personal jurisdiction over Plaintiff comports with the United States Constitution and is proper because Plaintiff has filed suit in this Court against Secure Computing asserting infringement of claims of the United States Patent No. 6,092,194. Venue within this judicial district is proper under Title 28, United States Code sections 1391(b), 1391(c) and/or 1400.

27. Plaintiff alleges that it is the owner of the United States Patent No. 6,092,194. Plaintiff contends that Secure Computing infringes claims of United States Patent No. 6,092,194.

28. United States Patent No. 6,092,194 and each claim thereof is invalid, unenforceable and not infringed by Secure Computing.

29. Secure Computing has not infringed any valid claims of U.S. Patent No. 6,092,194, either directly, indirectly, contributorily or otherwise, and have not induced any others to infringe said patent.

30. Secure Computing therefore seeks a declaration and finding by this Court that United States Patent No. 6,092,194 is invalid and unenforceable and that Secure Computing does not infringe, directly, indirectly, contributorily or otherwise, and has not induced any others to infringe, any valid claims of United States Patent No. 6,092,194.

PRAYER FOR RELIEF

WHEREFORE, Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG deny that Plaintiff is entitled to any relief for its Complaint and prays for judgment in Defendants' favor as prayed for in their Counterclaims and against Plaintiff as follows:

A. That Plaintiff take nothing by its Complaint and its claims against Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be dismissed with prejudice;

B. That Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be found not to infringe, either directly, indirectly, contributorily, or otherwise, and be found not to have induced infringement of any valid claims of United States Patent No. 6,092,194;

C. That United States Patent No. 6,092,194 be found invalid and unenforceable;

D. That Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be awarded costs, disbursements and attorneys' fees incurred in defending themselves in connection with the Complaint; and

E. That Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be awarded such other and further relief as the Court deems just, equitable and proper.

DEMAND FOR A JURY TRIAL

Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG hereby request a trial by jury, pursuant to Rule 38 of the Federal Rules of Civil Procedure, on all issues so triable.

Frederick L. Cottrell, III (#2555)
Cottrell@rlf.com
Matthew W. King (#4566)
king@rlf.com
Richards, Layton & Finger, P.A.
One Rodney Square
P.O. Box 551
Wilmington, DE 19899
(302) 651-7700
Attorneys For Defendants

Of Counsel:

Ronald J. Schutz
Jake M. Holdreith
Christopher A. Seidl
Trevor J. Foster
ROBINS, KAPLAN, MILLER & CIRESI L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

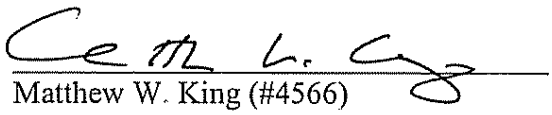
Dated: July 26, 2006

CERTIFICATE OF SERVICE

I hereby certify that on July 26, 2006, I electronically filed the foregoing with the Clerk of Court using CM/ECF which will send notification of such filing(s) to the following and which has also been served as noted:

BY HAND

Philip A. Rovner
Potter Anderson & Corroon LLP
1313 N. Market Street
Hercules Plaza, 6th Floor
P. O. Box 951
Wilmington, DE 19899-0951



Matthew W. King (#4566)
king@rlf.com

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation,	)	
Plaintiff,	)	Civil Action No. 06-369-GMS
v.	)	
SECURE COMPUTING CORPORATION, a Delaware corporation; CYBERGUARD CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100,	)	**DEMAND FOR JURY TRIAL**
Defendants.	)	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan Software, Ltd. ("Plaintiff" or "Finjan") alleges as follows:

THE PARTIES

1. Plaintiff Finjan is a corporation organized and existing under the laws of Israel, with its principal place of business at Hamachshev St. 1, New Industrial Area, Netanya, 42504, Israel.

2. On information and belief, Defendant Secure Computing Corporation ("Secure Computing") is a corporation organized and existing under the laws of the State of Delaware, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

3. On information and belief, Defendant Cyberguard Corporation ("Cyberguard") is a corporation organized and existing under the laws of the State of Delaware and a wholly owned subsidiary of Secure Computing, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

4. On information and belief, Defendant Webwasher AG ("Webwasher") is a corporation organized and existing under the laws of Germany and a wholly owned subsidiary of Cyberguard, with a branch office at 5201 Great America Parkway, Suite 432, Santa Clara, CA 95054.

JURISDICTION AND VENUE

5. This action arises under the Patent Act, 35 U.S.C. §271 *et seq.* This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§1331 and 1338.

6. Venue in this judicial district is proper under 28 U.S.C. §§ 1391 (b) and (c) and/or 28 U.S.C. § 1400(b). Personal jurisdiction over defendants comports with the United States Constitution and § 3104 of the Delaware Code because defendants are Delaware corporations and/or have and continue to infringe, contributorily infringe and/or induce the infringement of U.S. Patent No. 6,092,194, U.S. Patent No. 6,804,780 and U.S. Patent No. 7,058,822 in this district.

PLAINTIFF'S PATENT

7. On July 18, 2000, United States Patent No. 6,092,194 ("the '194 Patent"), entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, was issued to Shlomo Touboul. Finjan was assigned all ownership rights to the '194 Patent. A true and correct copy of the '194 Patent is attached to this complaint as Exhibit A and is incorporated by reference herein.

8. On October 12, 2004, United States Patent No. 6,804,780 ("the '780 Patent"), entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, was issued to Shlomo Touboul. Finjan was assigned all

ownership rights to the '780 Patent. A true and correct copy of the '780 Patent is attached to this complaint as Exhibit B and is incorporated by reference herein.

9. On June 6, 2006, United States Patent No. 7,058,822 ("the '822 Patent"), entitled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered and David R. Kroll. Finjan was assigned all ownership rights to the '822 Patent. A true and correct copy of the '822 Patent is attached to this complaint as Exhibit C and is incorporated by reference herein.

10. The '194 Patent, '780 Patent and '822 Patent are directed to a system and method for protecting networks and computers from hostile downloadable executable application programs.

PATENT INFRINGEMENT

11. On information and belief, defendant Secure Computing is in the business of developing and distributing network and systems security solutions to organizations. Secure Computing has and continues to infringe the '194 Patent, '780 Patent and '822 Patent by making, using, selling, distributing, advertising and marketing products, including but not limited to the Webwasher Secure Content Management ("SCM") suite, that infringe the '194 Patent, '780 Patent and '822 Patent.

12. On information and belief, defendant Cyberguard is in the business of developing and distributing information security solutions. Cyberguard has and continues to infringe the '194 Patent, '780 Patent and '822 Patent by making, using, selling, distributing, advertising and marketing products, including but not limited to the Webwasher Secure Content Management ("SCM") suite, that infringe the '194 Patent, '780 Patent and '822 Patent.

13. On information and belief, defendant Webwasher is in the business of developing and distributing Internet and email content security and filtering solutions. Webwasher has and

continues to infringe the '194 Patent, '780 Patent and '822 Patent by making, using, selling, distributing, advertising and marketing products, including but not limited to the Webwasher Secure Content Management ("SCM") suite, that infringe the '194 Patent, '780 Patent and '822 Patent.

FIRST CAUSE OF ACTION

(Infringement of the '194 Patent)

14. Finjan realleges each and every allegation set forth in Paragraphs 1 through 13, inclusive, and incorporates them herein by reference.

15. Defendants Secure Computing, Cyberguard and Webwasher have been and continue to infringe, contributorily infringe, and/or induce the infringement of the '194 Patent by making, using, selling and/or offering to sell products which infringe the '194 Patent, including but not limited to the Webwasher SCM suite, and will continue to do so until enjoined by this Court.

16. Defendants' infringement of the '194 Patent has been and continues to be willful and deliberate.

17. Defendants' infringement of the '194 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

SECOND CAUSE OF ACTION

(Infringement of the '780 Patent)

18. Finjan realleges each and every allegation set forth in Paragraphs 1 through 17, inclusive, and incorporates them herein by reference.

19. Defendants Secure Computing, Cyberguard and Webwasher have been and continue to infringe, contributorily infringe, and/or induce the infringement of the '780 Patent by making, using, selling and/or offering to sell products which infringe the '780 Patent, including but not limited to the Webwasher SCM suite, and will continue to do so until enjoined by this Court.

20. Defendants' infringement of the '780 Patent has been and continues to be willful and deliberate.

21. Defendants' infringement of the '780 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

THIRD CAUSE OF ACTION

(Infringement of the '822 Patent)

22. Finjan realleges each and every allegation set forth in Paragraphs 1 through 21, inclusive, and incorporates them herein by reference.

23. Defendants Secure Computing, Cyberguard and Webwasher have been and continue to infringe, contributorily infringe, and/or induce the infringement of the '822 Patent by making, using, selling and/or offering to sell products which infringe the '822 Patent, including but not limited to the Webwasher SCM suite, and will continue to do so until enjoined by this Court.

24. Defendants' infringement of the '822 Patent has been and continues to be willful and deliberate.

25. Defendants' infringement of the '822 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Finjan prays that the Court grant the following relief and judgment:

A. A preliminary and permanent injunction against Defendants Secure Computing, Cyberguard and Webwasher and its respective officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing, contributorily infringing, or inducing the infringement of the '194 Patent, '780 Patent and '822 Patent, and for all further and proper injunctive relief pursuant to 35 U.S.C. §283;

B. An award to Finjan of such damages as it shall prove at trial against Defendants Secure Computing, Cyberguard and Webwasher, that are adequate to fully compensate it for their infringement of the '194 Patent, '780 Patent and '822 Patent, said damages to be no less than a reasonable royalty;

C. An award to Finjan for willful infringement against Defendants Secure Computing, Cyberguard and Webwasher of three times the damages so determined, as provided by 35 U.S.C. §284, together with prejudgment interest from the date infringement of the '194 Patent, '780 Patent and/or '822 Patent began;

D. A finding that this case is "exceptional" and an award to Finjan of its costs and reasonable attorney's fees, as provided by 35 U.S.C. §285;

E. Such further and other relief as the Court and/or jury may deem proper and just.

DEMAND FOR JURY TRIAL

Plaintiff Finjan Software, Ltd. hereby demands a trial by jury on all issues triable by a jury.

POTTER ANDERSON & CORROON LLP

OF COUNSEL:

Paul J. Andre
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, California 94025-1114
(650) 838-4300

Dated: April 5, 2007
787724

By /s/ Philip A. Rovner
Philip A. Rovner (#3215)
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, Philip A. Rovner, hereby certify that on April 10, 2007, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

BY HAND DELIVERY

Frederick L. Cottrell, III, Esq.
Gregory E. Stuhlman, Esq.
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
cottrell@rlf.com;
stuhlman@rlf.com

I hereby certify that on April 10, 2007 I have sent by Federal Express the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.
Christopher A. Seidl, Esq.
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
jmholdreith@rkmc.com
caseidl@rkmc.com

/s/ Philip A. Rovner
Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P.O. Box 951
Wilmington, Delaware 19899
(302) 984-6000
E-mail: provner@potteranderson.com

EXHIBIT A

US006092194A

United States Patent [19]

Touboul

[11] **Patent Number: 6,092,194**

[45] **Date of Patent: *Jul. 18, 2000**

[54] **SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES**

[75] Inventor: **Shlomo Touboul**, Kefar-Haim, Israel

[73] Assignee: **Finjan Software, Ltd.**, Netanya, Israel

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/964,388**

[22] Filed: **Nov. 6, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/030,639, Nov. 8, 1996.

[51] **Int. Cl.**[7] **H04L 1/00**

[52] **U.S. Cl.** **713/200**

[58] **Field of Search** 395/187.01, 186; 713/200, 201, 202; 714/38, 704; 709/229

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,077,677	12/1991	Murphy et al.	395/10
5,361,359	11/1994	Tajalli et al.	395/700
5,485,409	1/1996	Gupta et al.	395/186
5,485,575	1/1996	Chess et al.	395/183.14
5,572,643	11/1996	Judson	395/793
5,623,600	4/1997	Ji et al.	395/187.01
5,638,446	6/1997	Rubin	380/25
5,692,047	11/1997	McManis	380/4
5,692,124	11/1997	Holden et al.	395/187.01
5,720,033	2/1998	Deo	395/186
5,724,425	3/1998	Chang et al.	380/25
5,740,248	4/1998	Fieres et al.	380/25
5,761,421	6/1998	van Hoff et al.	395/200.53
5,765,205	6/1998	Breslau et al.	711/203
5,784,459	7/1998	Devarakonda et al.	380/4
5,796,952	8/1998	Davis et al.	395/200.54
5,805,829	9/1998	Cohen et al.	395/200.32
5,832,208	11/1998	Chen et al.	395/187.01
5,850,559	12/1998	Angelo et al.	395/750.03
5,864,683	1/1999	Boebert et al.	395/200.79
5,892,904	4/1999	Atkinson et al.	395/187.01

OTHER PUBLICATIONS

Web page: http://iel.ihs.com:80/cgi-bin/iel_cgi?se...2ehts%26ViewTemplate%3ddocvie%5fb%2ehts, Okamato, E. et al., "ID-Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013-5194, Jul. 19, 1990, Abstract and pp. 1169-1170.

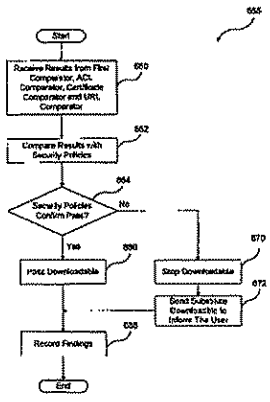
(List continued on next page.)

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Christopher Revak
Attorney, Agent, or Firm—Graham & James LLP

[57] **ABSTRACT**

A system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

68 Claims, 10 Drawing Sheets



OTHER PUBLICATIONS

"Finjan Announces a Personal Java ™ Firewall For Web Browsers—the SurfinShield™ 1.6", Press Release of Finjan Releases SurfinShield, Oct. 21, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software, Ltd., Jul. 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™"Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

"Company Profile Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavillion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Article published on the Internet, 7 pages.

Mark LaDue, "Online Business Consultant" Article published on the Internet, Home Page, Inc. 1996, 4 pages.

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, p 27, May 1990.

Norvin Leach et al, "IE 3.0 applets will earn certification", PC Week, v13, n29, p1(2), Jul. 1996.

Microsoft Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996.

Frequently Asked Questions About Authenticode, Microsoft Corporation, Feb. 1997.

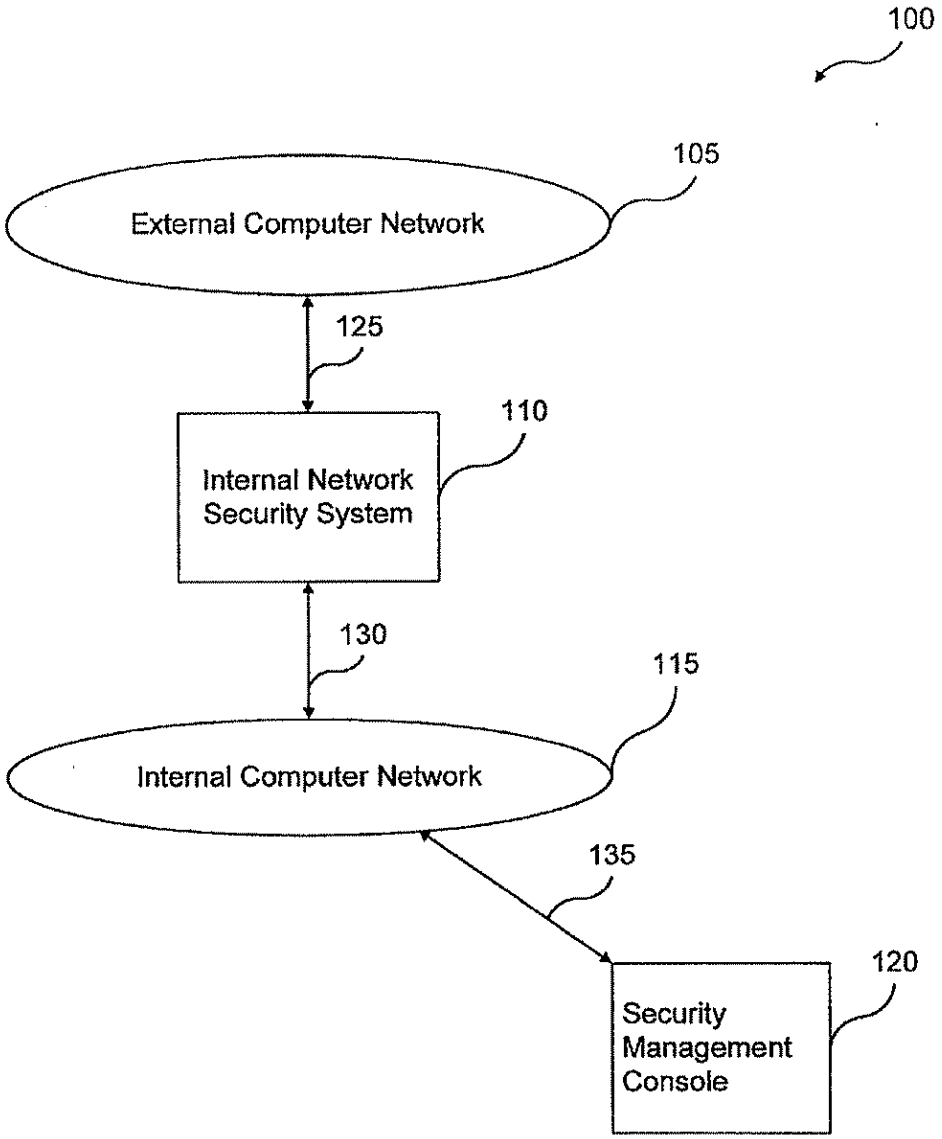

100
105
External Computer Network
125
110
Internal Network Security System
130
115
Internal Computer Network
135
120
Security Management Console

FIG. 1

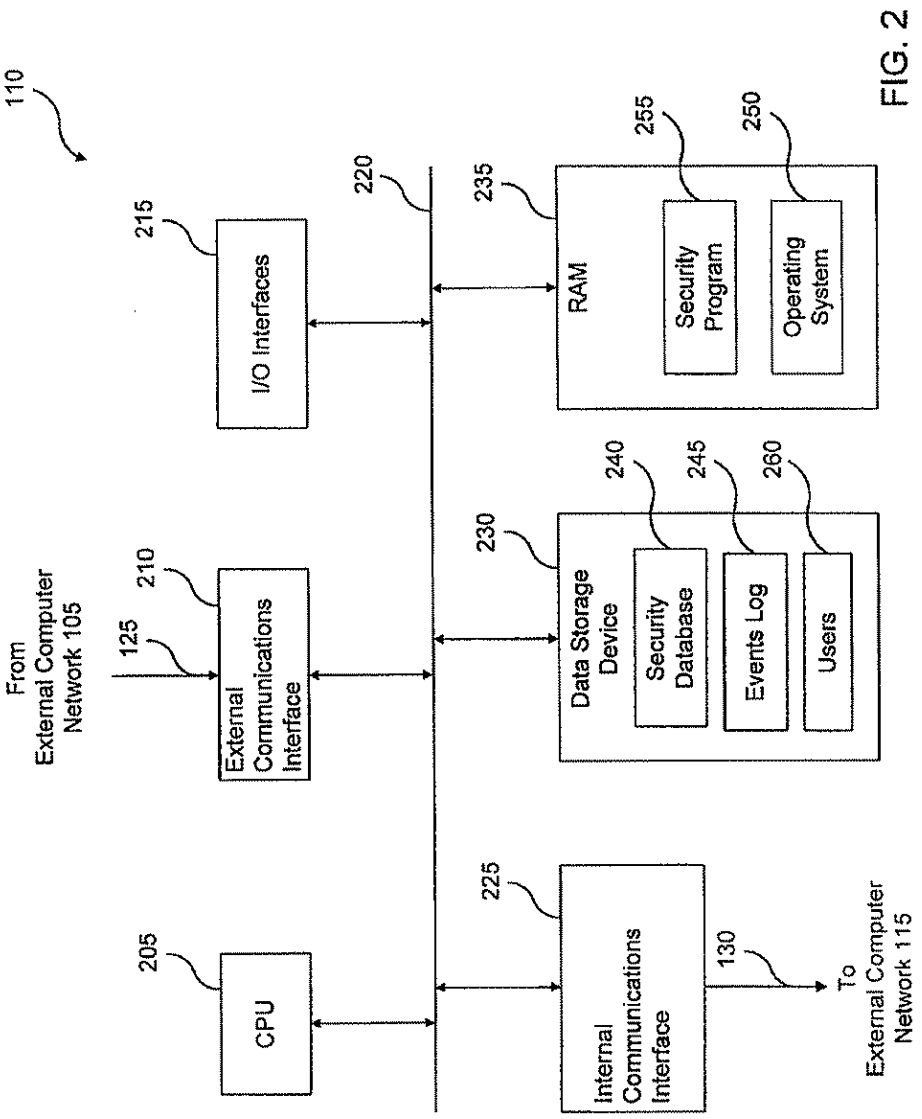

110
215
I/O Interfaces
220
235
RAM
255
Security Program
250
Operating System
From External Computer Network 105
125
210
External Communications Interface
230
Data Storage Device
240
Security Database
245
Events Log
260
Users
205
CPU
225
Internal Communications Interface
130
To External Computer Network 115

FIG. 2

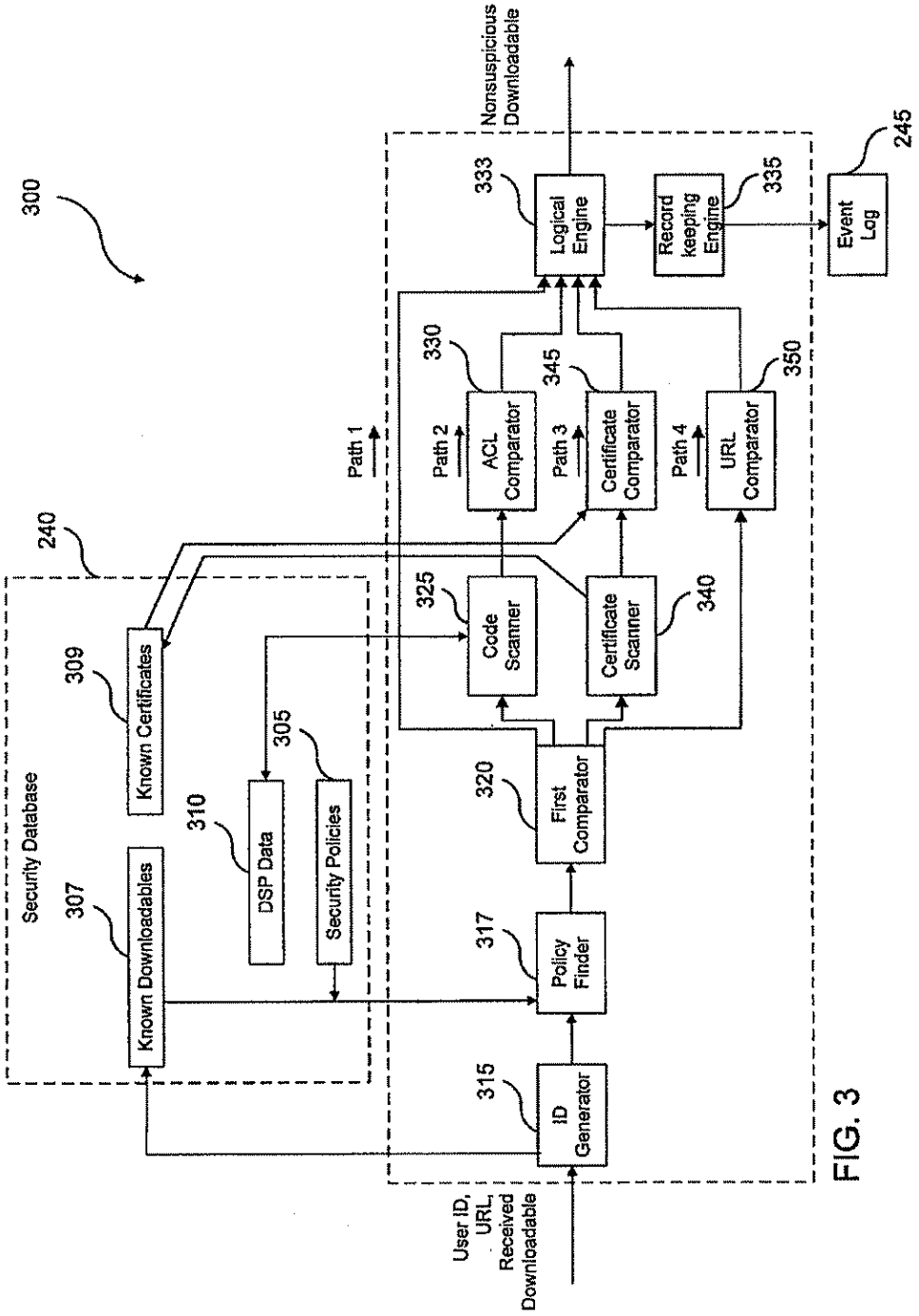

300
Nonsuspicious Downloadable
333
Logical Engine
Record keeping Engine
335
Event Log
245
330
345
350
Path 1
Path 2
ACL Comparator
Path 3
Certificate Comparator
Path 4
URL Comparator
240
325
Code Scanner
Certificate Scanner
340
309
Known Certificates
305
310
DSP Data
Security Policies
320
First Comparator
Security Database
307
Known Downloadables
317
Policy Finder
315
ID Generator
User ID, URL, Received Downloadable

FIG. 3

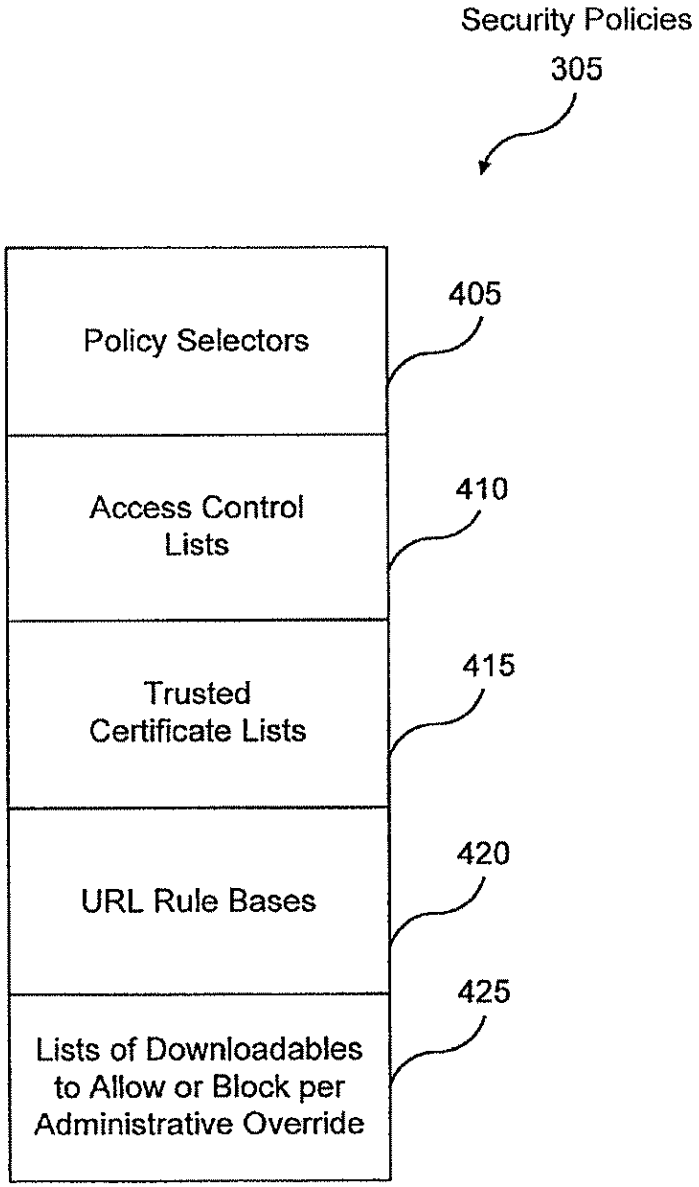

Security Policies
305
Policy Selectors
405
Access Control Lists
410
Trusted Certificate Lists
415
URL Rule Bases
420
Lists of Downloadables to Allow or Block per Administrative Override
425

FIG. 4

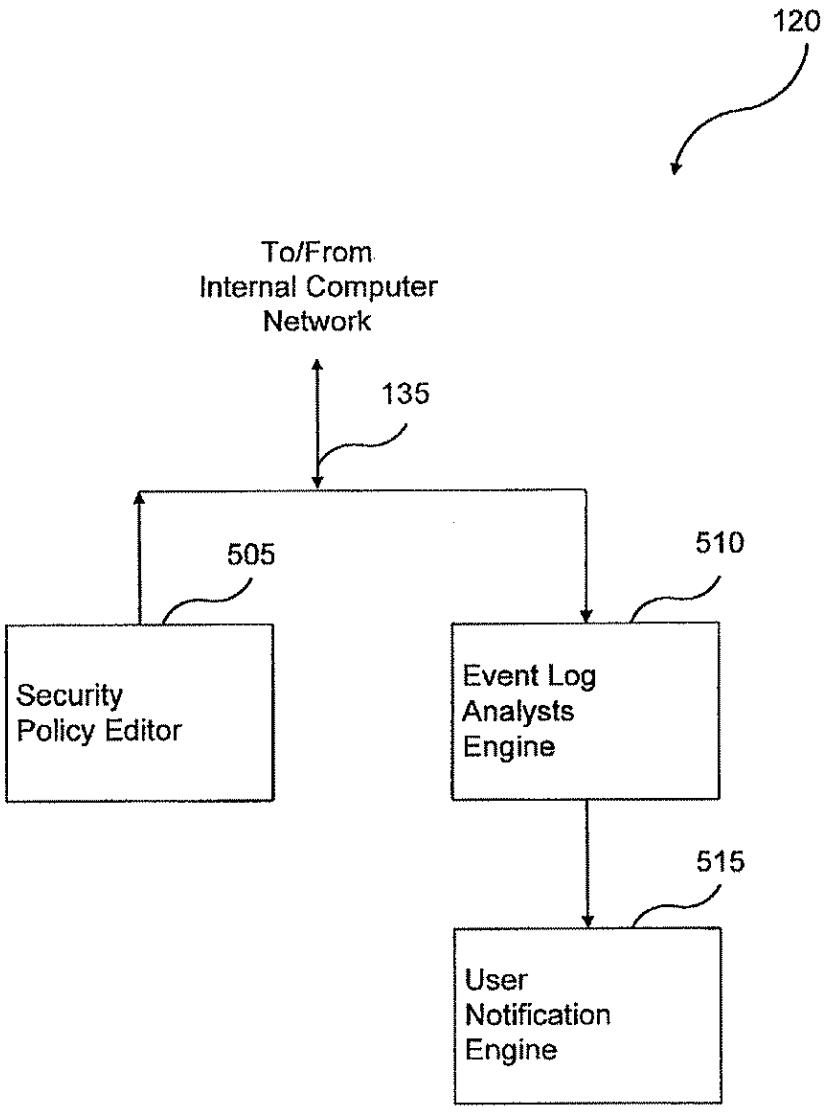

120
To/From
Internal Computer
Network
135
505
510
Security
Policy Editor
Event Log
Analysts
Engine
515
User
Notification
Engine

FIG. 5

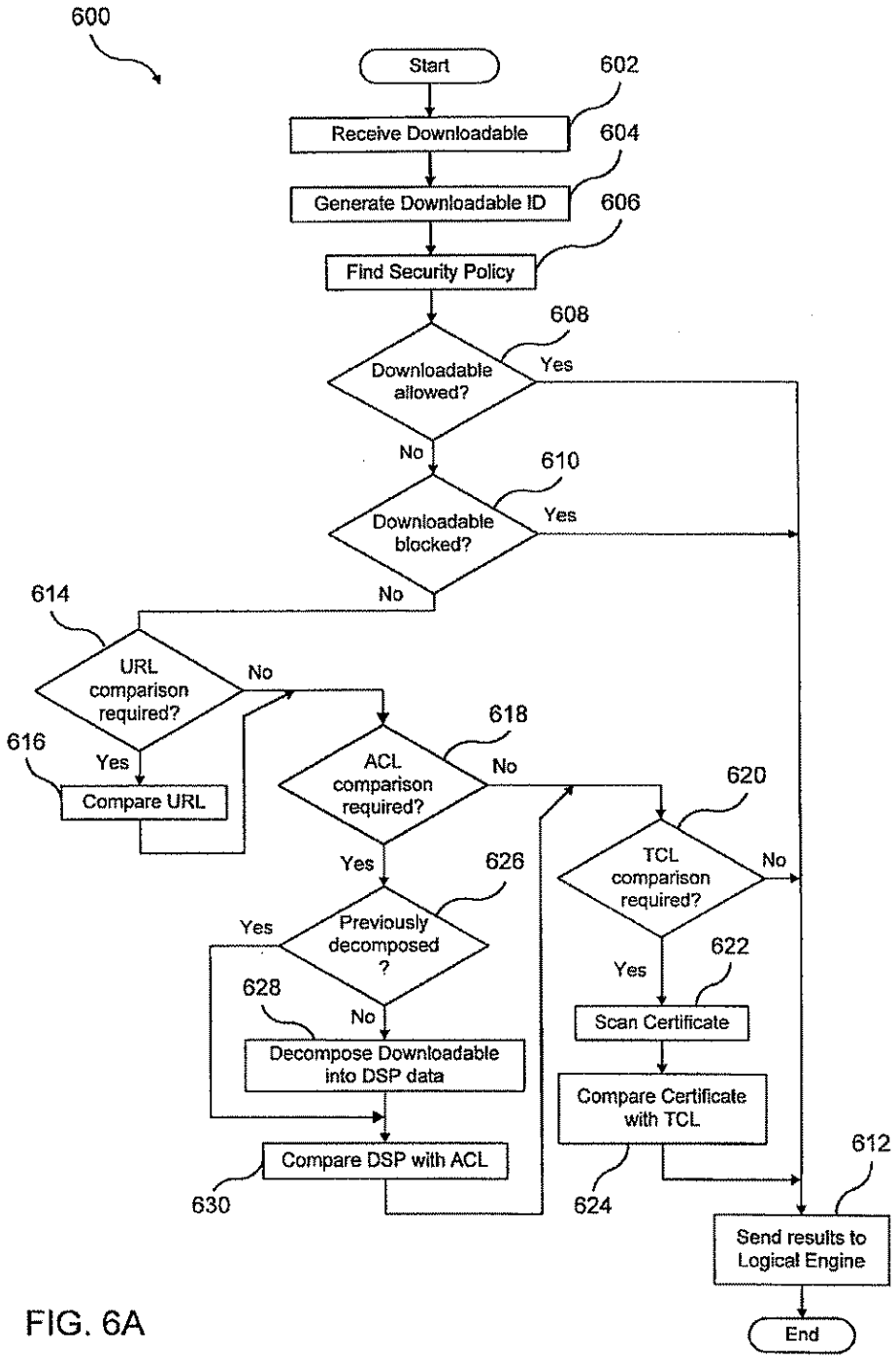

600
Start
602
Receive Downloadable
604
Generate Downloadable ID
606
Find Security Policy
608
Downloadable allowed?
Yes
No
610
Downloadable blocked?
Yes
No
614
URL comparison required?
No
616
Yes
Compare URL
618
ACL comparison required?
No
620
TCL comparison required?
No
Yes
626
Previously decomposed ?
Yes
628
No
Decompose Downloadable into DSP data
Compare DSP with ACL
630
622
Yes
Scan Certificate
Compare Certificate with TCL
624
612
Send results to Logical Engine
End

FIG. 6A

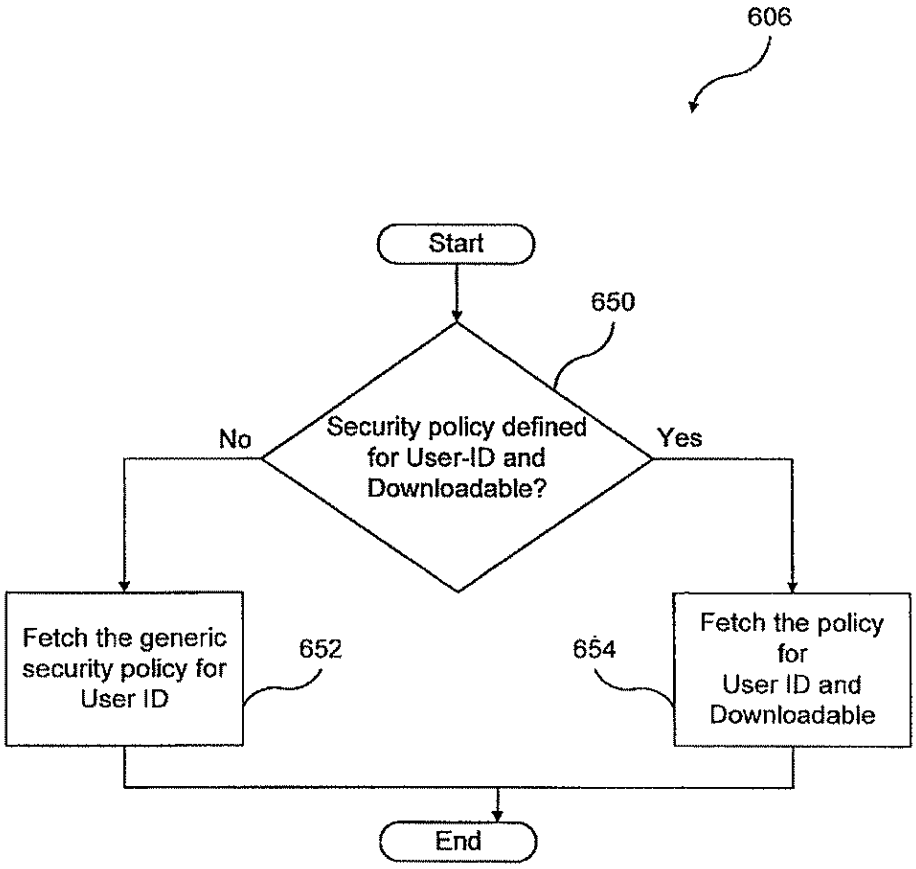

606
Start
650
Security policy defined for User-ID and Downloadable?
No
Yes
Fetch the generic security policy for User ID
652
654
Fetch the policy for User ID and Downloadable
End

FIG. 6B

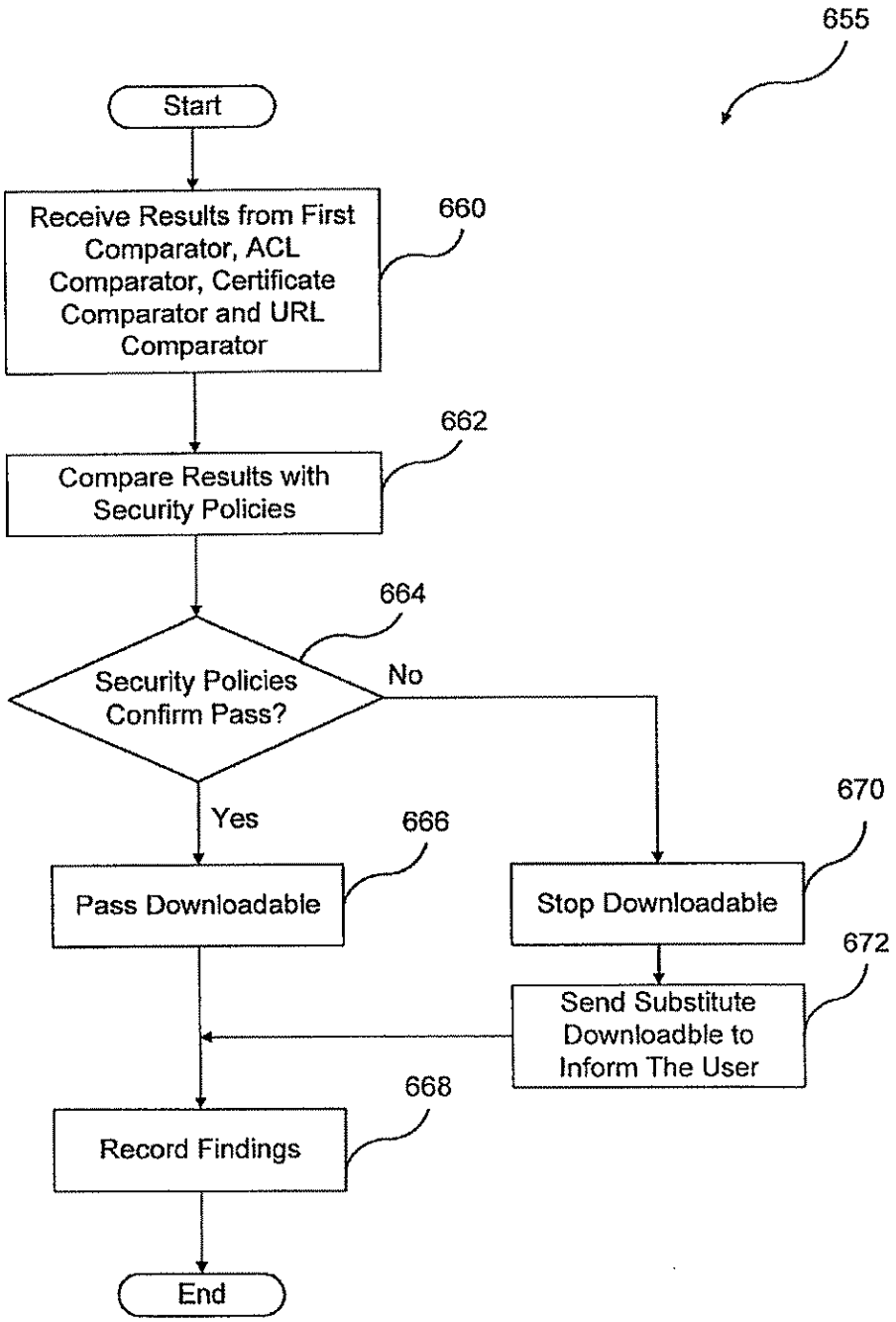

655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
664
Security Policies Confirm Pass?
No
Yes
666
Pass Downloadable
670
Stop Downloadable
672
Send Substitute Downloadble to Inform The User
668
Record Findings
End

FIG. 6C

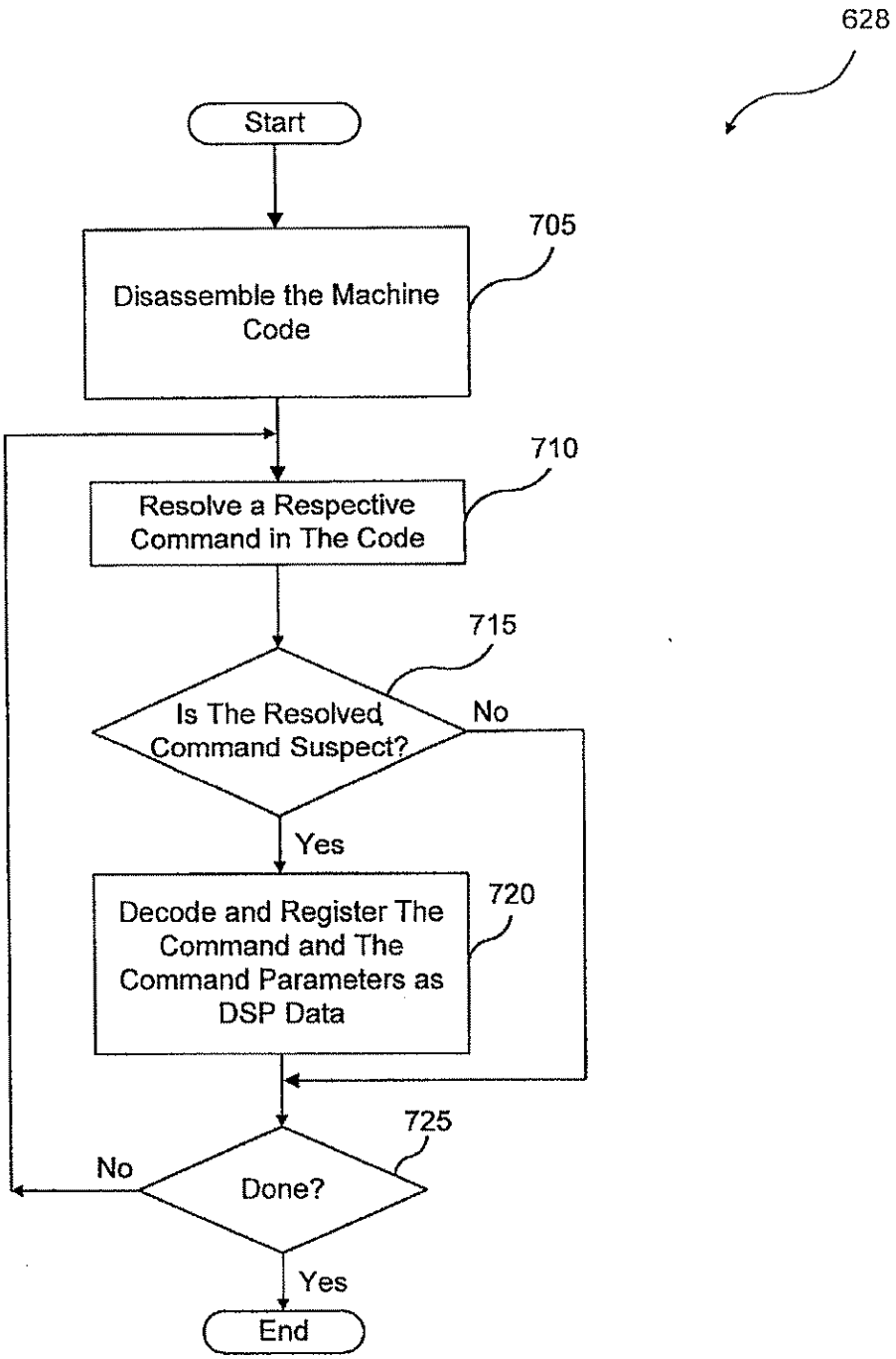

628
Start
705
Disassemble the Machine Code
710
Resolve a Respective Command in The Code
715
Is The Resolved Command Suspect?
No
Yes
720
Decode and Register The Command and The Command Parameters as DSP Data
725
Done?
No
Yes
End

FIG. 7

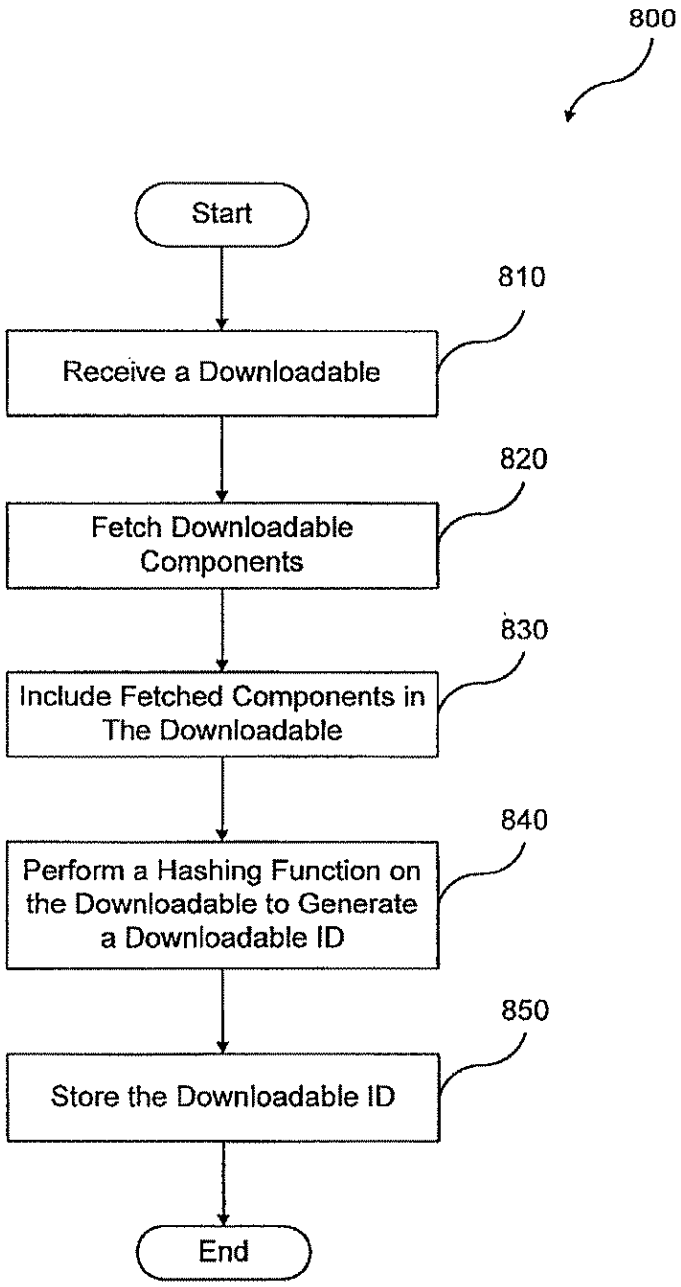

800
Start
810
Receive a Downloadable
820
Fetch Downloadable Components
830
Include Fetched Components in The Downloadable
840
Perform a Hashing Function on the Downloadable to Generate a Downloadable ID
850
Store the Downloadable ID
End

FIG. 8

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

INCORPORATION BY REFERENCE TO RELATED APPLICATION

This application hereby incorporates by reference related U.S. patent application Ser. No. 08/790,097, entitled "System and Method for Protecting a Client from Hostile Downloadables," filed on Jan. 29, 1997, by inventor Shlomo Touboul.

PRIORITY REFERENCE TO PROVISIONAL APPLICATION

This application claims benefit of and hereby incorporates by reference provisional application Ser. No. 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov. 8, 1996, by inventor Shlomo Touboul.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and method for protecting a computer and a network from hostile Downloadables.

2. Description of the Background Art

The Internet is currently a collection of over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate. Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

Accordingly, programmers continue to design computer and computer network security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as "Downloadables." A Downloadable is an executable application program, which is downloaded from a source computer and run on the destination computer. Downloadable is typically requested by an ongoing process such as by an Internet browser or web engine. Examples of Downloadables include Java™ applets designed for use in the Java™ distributing environment developed by Sun Microsystems, Inc., JavaScript scripts also developed by Sun Microsystems, Inc., ActiveX™ controls designed for use in the ActiveX™ distributing environment developed by the Microsoft Corporation, and Visual Basic also developed by the Microsoft Corporation. Therefore, a system and method are needed to protect a network from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a network from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The

security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied based on the client/group and on the particular Downloadable received. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components.

Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

The present invention further provides a method for protecting a computer from suspicious Downloadables. The method comprises the steps of receiving a Downloadable, comparing the Downloadable against a security policy to determine if the security policy has been violated, and discarding the Downloadable if the security policy has been violated.

It will be appreciated that the system and method of the present invention may provide computer protection from known hostile Downloadables. The system and method of the present invention may identify Downloadables that perform operations deemed suspicious. The system and method of the present invention may examine the Downloadable code to determine whether the code contains any suspicious operations, and thus may allow or block the Downloadable accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating a network system, in accordance with the present invention;

FIG. **2** is a block diagram illustrating details of the internal network security system of FIG. **1**;

FIG. **3** is a block diagram illustrating details of the security program and the security database of FIG. **2**;

FIG. **4** is a block diagram illustrating details of the security policies of FIG. **3**;

FIG. **5** is a block diagram illustrating details of the security management console of FIG. **1**;

FIG. **6**A is a flowchart illustrating a method of examining for suspicious Downloadables, in accordance with the present invention;

FIG. **6**B is a flowchart illustrating details of the step for finding the appropriate security policy of FIG. **6**A;

FIG. **6**C is a flowchart illustrating a method for determining whether an incoming Downloadable is to be deemed suspicious;

FIG. **7** is a flowchart illustrating details of the FIG. **6** step of decomposing a Downloadable; and

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a block diagram illustrating a network system **100**, in accordance with the present invention. The network

system **100** includes an external computer network **105**, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a communications channel **125** to an internal network security system **110**. The network system **100** further includes an internal computer network **115**, such as a corporate Local Area Network (LAN), coupled via a communications channel **130** to the internal network computer system **110** and coupled via a communications channel **135** to a security management console **120**.

The internal network security system **110** examines Downloadables received from external computer network **105**, and prevents Downloadables deemed suspicious from reaching the internal computer network **115**. It will be further appreciated that a Downloadable is deemed suspicious if it performs or may perform any undesirable operation, or if it threatens or may threaten the integrity of an internal computer network **115** component. It is to be understood that the term "suspicious" includes hostile, potentially hostile, undesirable, potentially undesirable, etc. Security management console **120** enables viewing, modification and configuration of the internal network security system **110**.

FIG. **2** is a block diagram illustrating details of the internal network security system **110**, which includes a Central Processing Unit (CPU) **205**, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a signal bus **220**. The internal network security system **110** further includes an external communications interface **210** coupled between the communications channel **125** and the signal bus **220** for receiving Downloadables from external computer network **105**, and an internal communications interface **225** coupled between the signal bus **220** and the communications channel **130** for forwarding Downloadables not deemed suspicious to the internal computer network **115**. The external communications interface **210** and the internal communications interface **225** may be functional components of an integral communications interface (not shown) for both receiving Downloadables from the external computer network **105** and forwarding Downloadables to the internal computer network **115**.

Internal network security system **110** further includes Input/Output (I/O) interfaces **215** (such as a keyboard, mouse and Cathode Ray Tube (CRT) display), a data storage device **230** such as a magnetic disk, and a Random-Access Memory (RAM) **235**, each coupled to the signal bus **220**. The data storage device **230** stores a security database **240**, which includes security information for determining whether a received Downloadable is to be deemed suspicious. The data storage device **230** further stores a users list **260** identifying the users within the internal computer network **115** who may receive Downloadables, and an event log **245** which includes determination results for each Downloadable examined and runtime indications of the internal network security system **110**. An operating system **250** controls processing by CPU **205**, and is typically stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution. A security program **255** controls examination of incoming Downloadables, and also may be stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution by CPU **205**.

FIG. **3** is a block diagram illustrating details of the security program **255** and the security database **240**. The security program **255** includes an ID generator **315**, a policy finder **317** coupled to the ID generator **315**, and a first comparator **320** coupled to the policy finder **317**. The first comparator **320** is coupled to a logical engine **333** via four separate paths, namely, via Path 1, via Path 2, via Path 3 and via Path 4. Path 1 includes a direct connection from the first comparator **320** to the logical engine **333**. Path 2 includes a code scanner coupled to the first comparator **320**, and an Access Control List (ACL) comparator **330** coupling the code scanner **325** to the logical engine **333**. Path 3 includes a certificate scanner **340** coupled to the first comparator **320**, and a certificate comparator **345** coupling the certificate scanner **340** to the logical engine **333**. Path 4 includes a Uniform Resource Locator (URL) comparator **350** coupling the first comparator **320** to the logical engine **3330**. A record-keeping engine **335** is coupled between the logical engine **333** and the event log **245**.

The security program **255** operates in conjunction with the security database **240**, which includes security policies **305**, known Downloadables **307**, known Certificates **309** and Downloadable Security Profile (DSP) data **310** corresponding to the known Downloadables **307**. Security policies **305** includes policies specific to particular users **260** and default (or generic) policies for determining whether to allow or block an incoming Downloadable. These security policies **305** may identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable. Referring to FIG. **4**, security policies **305** include policy selectors **405**, access control lists **410**, trusted certificate lists **415**, URL rule bases **420**, and lists **425** of Downloadables to allow or to block per administrative override.

Known Downloadables **307** include lists of Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, of Downloadables which OEMs know to be non-hostile, and of Downloadables previously received by this security program **255**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by each known Downloadable **307**, and may also include the respective arguments of these operations. An identified argument of an operation is referred to as "resolved." An unidentified argument is referred to as "unresolved." DSP data **310** is described below with reference to the code scanner **325**.

The ID generator **315** receives a Downloadable (including the URL from which it came and the userID of the intended recipient) from the external computer network **105** via the external communications interface **210**, and generates a Downloadable ID for identifying each Downloadable. The Downloadable ID preferably includes a digital hash of the complete Downloadable code. The ID generator **315** preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator **315** may prefetch all classes embodied in or identified by the Java™ applet bytecode to generate the Downloadable ID. Similarly, the ID generator **315** may retrieve all components listed in the .INF file for an ActiveX™ control to compute a Downloadable ID. Accordingly, the Downloadable ID for the Downloadable will be the same each time the ID generator **315** receives the same Downloadable. The ID generator **315** adds the generated Downloadable ID to the list of known Downloadables **307** (if it is not already listed). The ID generator **315** then forwards the Downloadable and Downloadable ID to the policy finder **317**.

The policy finder **317** uses the userID of the intended user and the Downloadable ID to select the specific security policy **305** that shall be applied on the received Downloadable. If there is a specific policy **305** that was defined for the user (or for one of its super groups) and the Downloadable, then the policy is selected. Otherwise the generic policy **305**

that was defined for the user (or for one of its super groups) is selected. The policy finder **317** then sends the policy to the first comparator **320**.

The first comparator **320** receives the Downloadable, the Downloadable ID and the security policy **305** from the policy finder **317**. The first comparator **320** examines the security policy **305** to determine which steps are needed for allowing the Downloadable. For example, the security policy **305** may indicate that, in order to allow this Downloadable, it must pass all four paths, Path 1, Path 2, Path 3 and Path 4. Alternatively, the security policy **305** may indicate that to allow the Downloadable, it must pass only one of the paths. The first comparator **320** responds by forwarding the proper information to the paths identified by the security policy **305**.

Path 1

In path 1, the first comparator **320** checks the policy selector **405** of the security policy **305** that was received from the policy finder **317**. If the policy selector **405** is either "Allowed" or "Blocked," then the first comparator **320** forwards this result directly to the logical engine **333**. Otherwise, the first comparator **320** invokes the comparisons in path 2 and/or path 3 and/or path 4 based on the contents of policy selector **405**. It will be appreciated that the first comparator **320** itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override **425**. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked."

Alternatively, the logical engine **333** may receive the results of each of the paths and based on the policy selector **405** may institute the final determination whether to allow or block the Downloadable. The first comparator **320** informs the logical engine **333** of the results of its comparison.

Path 2

In path 2, the first comparator **320** delivers the Downloadable, the Downloadable ID and the security policy **305** to the code scanner **325**. If the DSP data **310** of the received Downloadable is known, the code scanner **325** retrieves and forwards the information to the ACL comparator **330**. Otherwise, the code scanner **325** resolves the DSP data **310**. That is, the code scanner **325** uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data **310**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable **307**, and may also include the respective arguments of these operations. For example, DSP data **310** may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner **325** may generate the DSP data **310** as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner **325** may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker.

An Example List of Operations Deemed Potentially Hostile

File operations: READ a file, WRITE a file;

Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET;

Registry operations: READ a registry item, WRITE a registry item;

Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAD, KILL PROCESS/THREAD, CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc.; and

Resource usage thresholds: memory, CPU, graphics, etc.

In the preferred embodiment, the code scanner **325** performs a full-content inspection. However, for improved speed but reduced security, the code scanner **325** may examine only a portion of the Downloadable such as the Downloadable header. The code scanner **325** then stores the DSP data into DSP data **310** (corresponding to its Downloadable ID), and sends the Downloadable, the DSP data to the ACL comparator **330** for comparison with the security policy **305**.

The ACL comparator **330** receives the Downloadable, the corresponding DSP data and the security policy **305** from the code scanner **325**, and compares the DSP data against the security policy **305**. That is, the ACL comparator **330** compares the DSP data of the received Downloadable against the access control lists **410** in the received security policy **305**. The access control list **410** contains criteria indicating whether to pass or fail the Downloadable. For example, an access control list may indicate that the Downloadable fails if the DSP data includes a WRITE command to a system file. The ACL comparator **330** sends its results to the logical engine **333**.

Path 3

In path 3, the certificate scanner **340** determines whether the received Downloadable was signed by a certificate authority, such as VeriSign, Inc., and scans for a certificate embodied in the Downloadable. The certificate scanner **340** forwards the found certificate to the certificate comparator **345**. The certificate comparator **345** retrieves known certificates **309** that were deemed trustworthy by the security administrator and compares the found certificate with the known certificates **309** to determine whether the Downloadable was signed by a trusted certificate. The certificate comparator **345** sends the results to the logical engine **333**.

Path 4

In path 4, the URL comparator **350** examines the URL identifying the source of the Downloadable against URLs stored in the URL rule base **420** to determine whether the Downloadable comes from a trusted source. Based on the security policy **305**, the URL comparator **350** may deem the Downloadable suspicious if the Downloadable comes from an untrustworthy source or if the Downloadable did not come from a trusted source. For example, if the Downloadable comes from a known hacker, then the Downloadable may be deemed suspicious and presumed hostile. The URL comparator **350** sends its results to the logical engine **333**.

The logical engine **333** examines the results of each of the paths and the policy selector **405** in the security policy **305** to determine whether to allow or block the Downloadable. The policy selector **405** includes a logical expression of the results received from each of the paths. For example, the logical engine **333** may block a Downloadable if it fails any one of the paths, i.e., if the Downloadable is known hostile (Path 1), if the Downloadable may request suspicious operations (Path 2), if the Downloadable was not signed by a trusted certificate authority (Path 3), or if the Downloadable came from an untrustworthy source (Path 4). The logical engine **333** may apply other logical expressions according to the policy selector **405** embodied in the security policy **305**. If the policy selector **405** indicates that the Downloadable may pass, then the logical engine **333** passes the Downloadable to its intended recipient. Otherwise, if the policy selector **405** indicates that the Downloadable should be blocked, then the logical engine **333** forwards a non-hostile Downloadable to the intended recipient to inform the user

that internal network security system **110** discarded the original Downloadable. Further, the logical engine **333** forwards a status report to the record-keeping engine **335**, which stores the reports in event log **245** in the data storage device **230** for subsequent review, for example, by the MIS director.

FIG. **5** is a block diagram illustrating details of the security management console **120**, which includes a security policy editor **505** coupled to the communications channel **135**, an event log analysis engine **510** coupled between communications channel **135** and a user notification engine **515**, and a Downloadable database review engine **520** coupled to the communications channel **135**. The security management console **120** further includes computer components similar to the computer components illustrated in FIG. **2**.

The security policy editor **505** uses an I/O interface similar to I/O interface **215** for enabling authorized user modification of the security policies **305**. That is, the security policy editor **505** enables the authorized user to modify specific security policies **305** corresponding to the users **260**, the default or generic security policy **305**, the Downloadables to block per administrative override, the Downloadables to allow per administrative override, the trusted certificate lists **415**, the policy selectors **405**, the access control lists **410**, the URLs in the URL rule bases **420**, etc. For example, if the authorized user learns of a new hostile Downloadable, then the user can add the Downloadable to the Downloadables to block per system override.

The event log analysis engine **510** examines the status reports contained in the event log **245** stored in the data storage device **230**. The event log analysis engine **510** determines whether notification of the user (e.g., the security system manager or MIS director) is warranted. For example, the event log analysis engine **510** may warrant user notification whenever ten (10) suspicious Downloadables have been discarded by internal network security system **110** within a thirty (30) minute period, thereby flagging a potential imminent security threat. Accordingly, the event log analysis engine **510** instructs the user notification engine **515** to inform the user. The user notification engine **515** may send an e-mail via internal communications interface **220** or via external communications interface **210** to the user, or may display a message on the user's display device (not shown).

FIG. **6A** is a flowchart illustrating a method **600** for protecting an internal computer network **115** from suspicious Downloadables. Method **600** begins with the ID generator **315** in step **602** receiving a Downloadable. The ID generator **315** in step **604** generates a Downloadable ID identifying the received Downloadable, preferably, by generating a digital hash of the Downloadable code (including prefetched components). The policy finder **317** in step **606** finds the appropriate security policy **305** corresponding to the userID specifying intended recipient (or the group to which the intended recipient belongs) and the Downloadable. The selected security policy **305** may be the default security policy **305**. Step **606** is described in greater detail below with reference to FIG. **6B**.

The first comparator **320** in step **608** examines the lists of Downloadables to allow or to block per administrative override **425** against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically. If so, then in step **612** the first comparator **320** sends the results to the logical engine **333**. If not, then the method **600** proceeds to step **610**. In step **610**, the first comparator **620** examines the lists of Downloadables to block per administrative override **425** against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically. If so, then the first comparator **420** in step **612** sends the results to the logical engine **333**. Otherwise, method **600** proceeds to step **614**.

In step **614**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 4. If not, then method **600** jumps to step **618**. If so, then the URL comparator **350** in step **616** compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases **420**, and then method **600** proceeds to step **618**.

In step **618**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 2. If not, then method **600** jumps to step **620**. Otherwise, the code scanner **235** in step **626** examines the DSP data **310** based on the Downloadable ID of the incoming Downloadable to determine whether the Downloadable has been previously decomposed. If so, then method **600** jumps to step **630**. Otherwise, the code scanner **325** in step **628** decomposes the Downloadable into DSP data. Downloadable decomposition is described in greater detail with reference to FIG. **7**. In step **630**, the ACL comparator **330** compares the DSP data of the incoming Downloadable against the access control lists **410** (which include the criteria necessary for the Downloadable to fail or pass the test).

In step **620**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 3. If not, then method **600** returns to step **612** to send the results of each of the test performed to the logical engine **333**. Otherwise, the certificate scanner **622** in step **622** scans the Downloadable for an embodied certificate. The certificate comparator **345** in step **624** retrieves trusted certificates from the trusted certificate lists (TCL) **415** and compares the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source. Method **600** then proceeds to step **612** by the certificate scanner **345** sending the results of each of the paths taken to the logical engine **333**. The operations of the logical engine **333** are described in greater detail below with reference to FIG. **6C**. Method **600** then ends.

One skilled in the art will recognize that the tests may be performed in a different order, and that each of the tests need not be performed. Further, one skilled in the art will recognize that, although path 1 is described in FIG. **6A** as an automatic allowance or blocking, the results of Path 1 may be another predicate to be applied by the logical engine **333**. Further, although the tests are shown serially in FIG. **6A**, the tests may be performed in parallel as illustrated in FIG. **3**.

FIG. **6B** is a flowchart illustrating details of step **606** of FIG. **6A** (referred to herein as method **606**). Method **606** begins with the policy finder **317** in step **650** determining whether security policies **305** include a specific security policy corresponding to the userID and the Downloadable. If so, then the policy finder **317** in step **654** fetches the corresponding specific policy **305**. If not, then the policy finder **317** in step **652** fetches the default or generic security policy **305** corresponding to the userID. Method **606** then ends.

FIG. **6C** is a flowchart illustrating details of a method **655** for determining whether to allow or to block the incoming Downloadable. Method **655** begins with the logical engine **333** in step **660** receiving the results from the first comparator **320**, from the ACL comparator **330**, from the certificate

comparator **345** and from the URL comparator **350**. The logical engine **333** in step **662** compares the results with the policy selector **405** embodied in the security policy **305**, and in step **664** determines whether the policy selector **405** confirms the pass. For example, the policy selector **405** may indicate that the logical engine **333** pass the Downloadable if it passes one of the tests of Path 1, Path 2, Path 3 and Path 4. If the policy selector **405** indicates that the Downloadable should pass, then the logical engine **333** in step **666** passes the Downloadable to the intended recipient. In step **668**, the logical engine **333** sends the results to the record-keeping engine **335**, which in turn stores the results in the event log **245** for future review. Method **655** then ends. Otherwise, if the policy selector **405** in step **664** indicates that the Downloadable should not pass, then the logical engine **333** in step **670** stops the Downloadable and in step **672** sends a non-hostile substitute Downloadable to inform the user that the incoming Downloadable has been blocked. Method **655** then jumps to step **668**.

FIG. **7** is a flowchart illustrating details of step **628** of FIG. **6**A (referred to herein as method **628**) for decomposing a Downloadable into DSP data **310**. Method **628** begins in step **705** with the code scanner **325** disassembling the machine code of the Downloadable. The code scanner **325** in step **710** resolves a respective command in the machine code, and in step **715** determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. **3**). If not, then the code scanner **325** in step **725** determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method **628** ends. Otherwise, method **628** returns to step **710**.

Otherwise, if the code scanner **325** in step **715** determines that the resolved command is suspect, then the code scanner **325** in step **720** decodes and registers the suspicious command and its command parameters as DSP data **310**. The code scanner **325** in step **720** registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method **628** then jumps to step **725**.

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable. Method **800** begins with the ID generator **315** in step **810** receiving a Downloadable from the external computer network **105**. The ID generator **315** in step **820** may fetch some or all components referenced in the Downloadable code, and in step **830** includes the fetched components in the Downloadable code. The ID generator **315** in step **840** performs a hashing function on at least a portion of the Downloadable code to generate a Downloadable ID. The ID generator **315** in step **850** stores the generated Downloadable ID in the security database **240** as a reference to the DSP data **310**. Accordingly, the Downloadable ID will be the same for the identical Downloadable each time it is encountered.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method, comprising the steps of:

receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client;

comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and

preventing execution of the Downloadable by the client if the security policy has been violated.

2. The method of claim **1**, further comprising the step of decomposing the Downloadable into the Downloadable security profile data.

3. The method of claim **2**, wherein the security policy includes an access control list and further comprising the step of comparing the Downloadable security profile data against the access control list.

4. The method of claim **1**, further comprising the steps of scanning for a certificate and comparing the certificate against a trusted certificate.

5. The method of claim **1**, further comprising the step of comparing the URL from which the Downloadable originated against a known URL.

6. The method of claim **5**, wherein the known URL is a trusted URL.

7. The method of claim **5**, wherein the known URL is an untrusted URL.

8. The method of claim **1**, wherein the Downloadable includes a Java™ applet.

9. The method of claim **1**, wherein the Downloadable includes an ActiveX™ control.

10. The method of claim **1**, wherein the Downloadable includes a JavaScript™ script.

11. The method of claim **1**, wherein the Downloadable includes a Visual Basic script.

12. The method of claim **1**, wherein

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

13. The method of claim **1**, wherein

the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

14. The method of claim **1**, wherein

the client belongs to a particular group; and

the security policy includes a specific security policy corresponding to the particular group.

15. The method of claim **1**, further comprising, after preventing execution of the Downloadable, the step of sending a substitute non-hostile Downloadable to the client for informing the client.

16. The method of claim **1**, further comprising, after preventing execution of the Downloadable, the step of recording the violation in an event log.

17. The method of claim **1**, further comprising the step of computing a Downloadable ID to identify the Downloadable.

18. The method of claim **16**, further comprising the steps of fetching components identified by the Downloadable and including the fetched components in the Downloadable.

19. The method of claim 18, further comprising the step of performing a hashing function on the Downloadable to compute a Downloadable ID to identify the Downloadable.

20. The method of claim 18, further comprising the step of fetching all components identified by the Downloadable.

21. The method of claim 1 further comprising the step of examining the intended recipient userID to determine the appropriate security policy.

22. The method of claim 20, wherein the appropriate security policy includes a default security policy.

23. The method of claim 1, further comprising the step of examining the Downloadable to determine the appropriate security policy.

24. The method of claim 1, further comprising the step of comparing the Downloadable against a known Downloadable.

25. The method of claim 24, wherein the known Downloadable is hostile.

26. The method of claim 24, wherein the known Downloadable is non-hostile.

27. The method of claim 24, further comprising the step of including a previously received Downloadable as a known Downloadable.

28. The method of claim 27, wherein the security policy identifies a Downloadable to be blocked per administrative override.

29. The method of claim 28, wherein the security policy identifies a Downloadable to be allowed per administrative override.

30. The method of claim 1, further comprising the step of informing a user upon detection of a security policy violation.

31. The method of claim 1, further comprising the steps of recognizing the incoming Downloadable, and obtaining the Downloadable security profile data for the incoming Downloadable from memory.

32. A system for execution by a server that serves as a gateway to a client, the system comprising:

a security policy;

an interface for receiving an incoming Downloadable addressed to a client;

a comparator, coupled to the interface, for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against the security policy to determine if the security policy has been violated; and

a logical engine for preventing execution of the Downloadable by the client if the security policy has been violated.

33. The system of claim 32, wherein the Downloadable includes a Java™ applet.

34. The system of claim 32, wherein the Downloadable includes ActiveX™ control.

35. The system of claim 32, wherein the Downloadable includes a JavaScript™ script.

36. The system of claim 32, wherein the Downloadable includes a Visual Basic script.

37. The system of claim 32, wherein

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

38. The system of claim 32, wherein

the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

39. The system of claim 32, wherein

the client belongs to a particular group; and

the security policy includes a specific security policy corresponding to the particular group.

40. The system of claim 32, further comprising an ID generator coupled to the interface for computing a Downloadable ID identifying the Downloadable.

41. The system of claim 40, wherein the ID generator prefetches all components of the Downloadable and uses all components to compute the Downloadable ID.

42. The system of claim 41, wherein the ID generator computes the digital hash of all the prefetched components.

43. The system of claim 32, further comprising a policy finder for finding the security policy.

44. The system of claim 43, wherein the policy finder finds the security policy based on the user.

45. The system of claim 43 wherein the policy finder finds the security policy based on the user and the Downloadable.

46. The system of claim 43, wherein the policy finder obtains the default security policy.

47. The system of claim 32 wherein the comparator examines the security policy to determine which tests to apply.

48. The system of claim 47 wherein the comparator compares the Downloadable against a known Downloadable.

49. The system of claim 48, wherein the known Downloadable is hostile.

50. The system of claim 48, wherein the known Downloadable is non-hostile.

51. The system of claim 32, wherein the security policy identifies a Downloadable to be blocked per administrative override.

52. The system of claim 32, wherein the security policy identifies a Downloadable to be allowed per administrative override.

53. The system of claim 32, wherein

the comparator sends a substitute non-hostile Downloadable to the client for informing the client.

54. The system of claim 32, further comprising a code scanner coupled to the comparator for decomposing the Downloadable into the Downloadable security profile data.

55. The system of claim 54, further comprising an ACL comparator coupled to the code scanner for comparing the Downloadable security profile data against an access control list.

56. The system of claim 32, further comprising a certificate scanner coupled to the comparator for examining the Downloadable for a certificate.

57. The system of claim 56, further comprising a certificate comparator coupled to the certificate scanner for comparing the certificate against a trusted certificate.

58. The system of claim 32, further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL.

59. The system of claim 58, wherein the known URL identifies an untrusted URL.

60. The system of claim 58, wherein the known URL identifies a trusted URL.

61. The system of claim 31, wherein the logical engine responds according to the security policy.

62. The system of claim 31, further comprising a record-keeping engine coupled to the comparator for recording results in an event log.

63. The system of claim 32, further comprising memory storing the Downloadable security profile data for the incoming Downloadable.

64. A system for execution on a server that serves as a gateway to a client, comprising:

means for receiving an incoming Downloadable addressed to a client;

means for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and

means for preventing execution of the Downloadable by the client if the security policy has been violated.

65. A computer-readable storage medium storing program code for causing a server that serves as a gateway to a client to perform the steps of:

receiving an incoming Downloadable addressed to a client;

comparing Downloadable security profile data pertaining to the Downloadable against a security policy to determine if the security policy has been violated; and

preventing execution of the Downloadable by the client if the security policy has been violated.

66. A method, comprising:

receiving a Downloadable;

decomposing the Downloadable into Downloadable security profile data; the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable,

comparing the Downloadable security profile data against a security policy; and

preventing execution of the Downloadable if the Downloadable security profile data violates the security policy.

67. The method of claim 66, further comprising:

fetching all components referenced by the Downloadable;

performing a hashing function of the Downloadable and the components fetched to compute a Downloadable ID; and

storing the Downloadable security profile data and the Downloadable ID in memory.

68. A method, comprising:

providing memory storing known-Downloadable security profile data and a that includes a list a suspicious computer operations that may be attempted by a Downloadable known-Downloadable ID corresponding to the Downloadable security profile data;

receiving an incoming Downloadable;

fetching all components referenced by the incoming Downloadable;

performing a hashing function of the Downloadable and the components to compute an incoming-Downloadable ID;

comparing the known-Downloadable ID against the incoming-Downloadable ID;

retrieving the Downloadable security profile data if the known-Downloadable ID and the incoming-Downloadable ID match; and

comparing the Downloadable security profile data against a security policy to determine if the incoming Downloadable violates the security policy.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,092,194
DATED : July 18, 2000
INVENTOR(S) : Shlomo Touboul

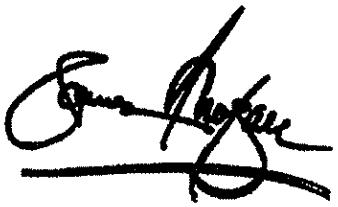
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 13,
Line 19, after "to the Downloadable" and before "against a security" insert --, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, --

Column 14,
Line 12, after "profile data and" and before "that includes" delete -- a --

Signed and Sealed this

Fifth Day of February, 2002



Attest:

Attesting Officer

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

EXHIBIT B

US006804780B1

(12) **United States Patent**
Touboul

(10) **Patent No.: US 6,804,780 B1**
(45) **Date of Patent: *Oct. 12, 2004**

(54) **SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES**

(75) Inventor: **Shlomo Touboul**, Kefar-haim (IL)

(73) Assignee: **Finjan Software, Ltd.**, Netanya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/539,667**

(22) Filed: **Mar. 30, 2000**

Related U.S. Application Data

(63) Continuation of application No. 08/964,388, filed on Nov. 6, 1997, now Pat. No. 6,092,194.
(60) Provisional application No. 60/030,639, filed on Nov. 8, 1996.

(51) **Int. Cl.**[7] **H04L 9/00**; G06F 11/30
(52) **U.S. Cl.** **713/181**; 713/201; 713/176; 717/178
(58) **Field of Search** 713/200, 201, 713/176, 181; 709/223, 225, 227, 229; 717/168–178

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,077,677	A	12/1991	Murphy et al.	
5,359,659	A	10/1994	Rosenthal	
5,361,359	A	11/1994	Tajalli et al.	
5,485,409	A	1/1996	Gupta et al.	
5,485,575	A	1/1996	Chess et al.	
5,572,643	A	11/1996	Judson	
5,579,509	A *	11/1996	Furtney et al.	703/27
5,606,668	A	2/1997	Shwed	
5,623,600	A	4/1997	Ji et al.	
5,638,446	A	6/1997	Rubin	
5,692,047	A	11/1997	McManis	
5,692,124	A	11/1997	Holden et al.	
5,720,033	A	2/1998	Deo	
5,724,425	A	3/1998	Chang et al.	
5,740,248	A	4/1998	Fieres et al.	
5,761,421	A	6/1998	van Hoff et al.	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

EP	1091276 A1 *	4/2001	G06F/1/00
EP	1132796 A1 *	9/2001	G06F/1/00

OTHER PUBLICATIONS

Khare, "Microsoft Authenticode Analyzed" Jul. 22, 1996, xent.com/FoRK-archive/summer96/0338.html, p. 1–2.*

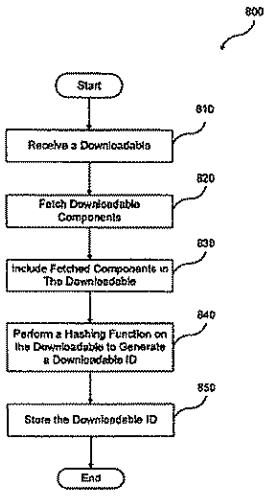
(List continued on next page.)

Primary Examiner—Ayaz Sheikh
Assistant Examiner—Christopher Revak
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey, L.L.P.

(57) **ABSTRACT**

A computer-based method for generating a Downloadable ID to identify a Downloadable, including obtaining a Downloadable that includes one or more references to software components required by the Downloadable, fetching at least one software component identified by the one or more references, and performing a function on the Downloadable and the fetched software components to generate a Downloadable ID. A system and a computer-readable storage medium are also described and claimed.

18 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

5,765,205	A		6/1998	Breslau et al.
5,784,459	A		7/1998	Devarakonda et al.
5,796,952	A		8/1998	Davis et al.
5,805,829	A		9/1998	Cohen et al.
5,832,208	A		11/1998	Chen et al.
5,832,274	A	*	11/1998	Cutler et al. 717/171
5,850,559	A		12/1998	Angelo et al.
5,859,966	A		1/1999	Hayman et al.
5,864,683	A		1/1999	Boebert et al.
5,892,904	A		4/1999	Atkinson et al.
5,951,698	A		9/1999	Chen et al.
5,956,481	A		9/1999	Walsh et al.
5,974,549	A		10/1999	Golan
5,978,484	A	*	11/1999	Apperson et al. 705/54
5,983,348	A		11/1999	Ji
6,092,194	A	*	7/2000	Touboul 713/200
6,154,844	A	*	11/2000	Touboul et al. 713/201
6,339,829	B1	*	1/2002	Beadle et al. 713/201

OTHER PUBLICATIONS

"Release Notes for the Microsfot ActiveX Development Kit", Aug. 13, 1996, activex.adsp.or.jp/inetsdk/readme.txt, p. 1–10.*

"Microsoft ActiveX Software Development Kit" Aug. 12, 1996, activex.adsp.or.jp/inetsdk/help/overview.htm, p. 1–6.*

Doyle et al, "Microsoft Press Computer Dictionary" 1993, Microsoft Press, 2nd Edition, p. 137–138.*

Schmitt, ".EXE. files, OS–2 style" Nov. 1988, PC Tech Journal via dialog search, vol. 6, #11, p. 76–78.*

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990; pp. 21–29.

Okamoto, E. et al., "ID–Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013/5194, Jul. 19, 1990, Abstract and pp. 1169–1170. URL: http://iel.ihs.com:80/cgi–bin/iel_cgi?se . . . 2ehts%26ViewTemplate%3ddocview%5fb%2ehts.

IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, Nov. 15, 1995, pp. 6–7.

Norvin Leach et al, "IE 3.0 Applets Will Earn Certification", PC Week, vol. 13, No. 29, Jul. 22, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Softwre Ltd., Jul. 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996, including Abstract, Contents, Introduction and pp. 1–10.

"Finjan Announces a Personal Java™ Firewall For Web Browsers—the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, Oct. 21, 1996, 2 pages.

Company Profile "Finjan—Safe Surfing, The Java Security Solutions Provider", Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Article published on the Internet, 7 pages.

Mark LaDue, "Online Business Consulant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.

Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated Feb. 17, 1997, Printed Dec. 23, 1998. URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9, pp. 1–13.

Zhang, X.N., "Secure Code Distribution", IEEE/IEE Electronic Library online, Computer, vol. 30, Issue 6, Jun., 1997, pp. 76–79.

* cited by examiner

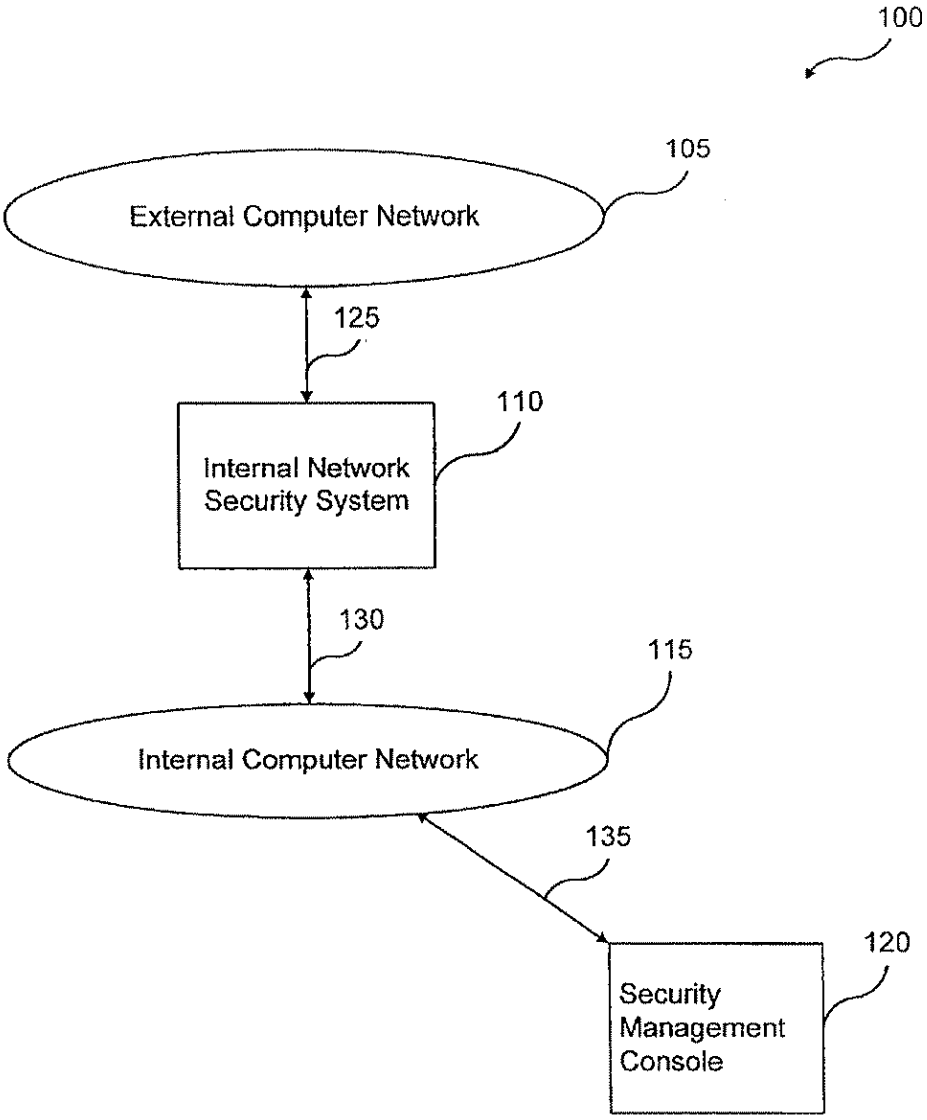

100
105
External Computer Network
125
110
Internal Network Security System
130
115
Internal Computer Network
135
120
Security Management Console

FIG. 1

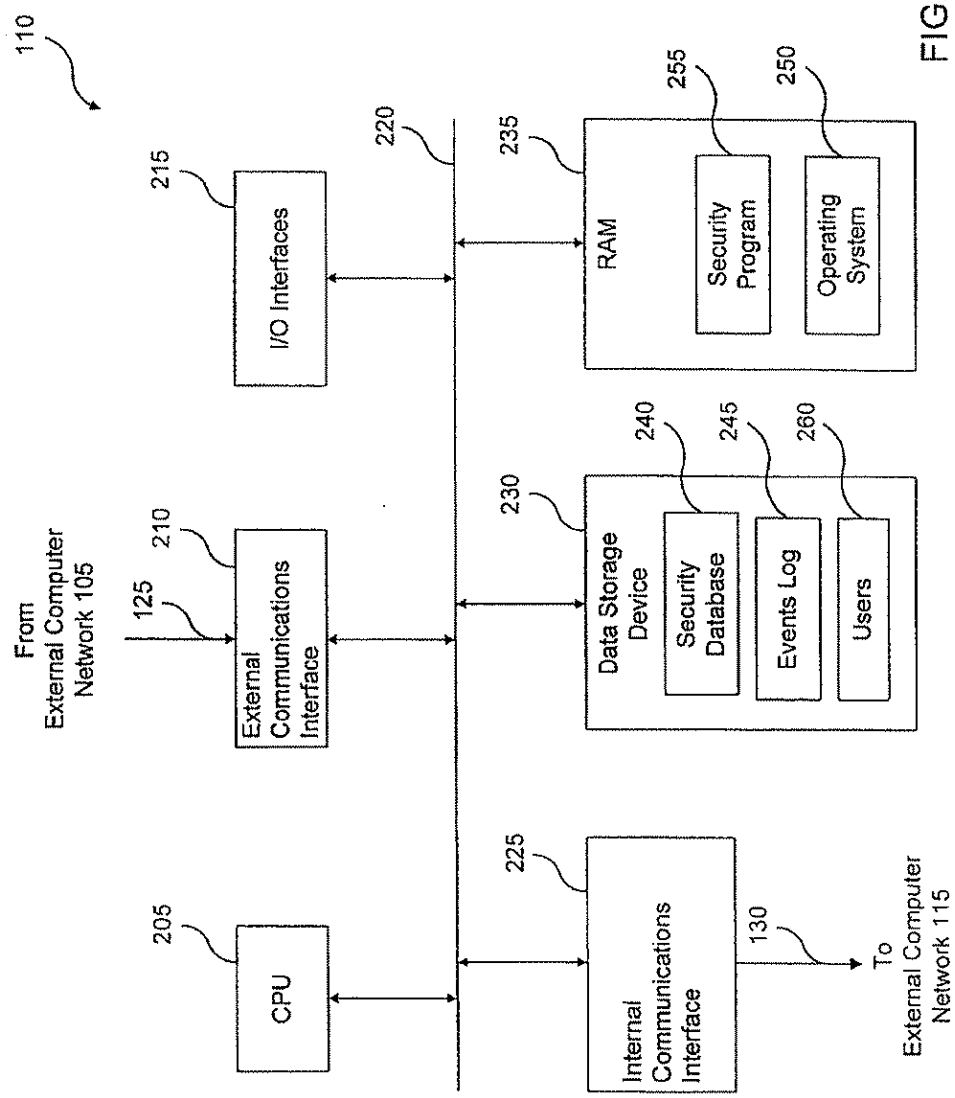

110
215
I/O Interfaces
220
235
RAM
255
Security Program
250
Operating System
From External Computer Network 105
125
210
External Communications Interface
230
Data Storage Device
240
Security Database
245
Events Log
260
Users
205
CPU
225
Internal Communications Interface
130
To External Computer Network 115

FIG. 2

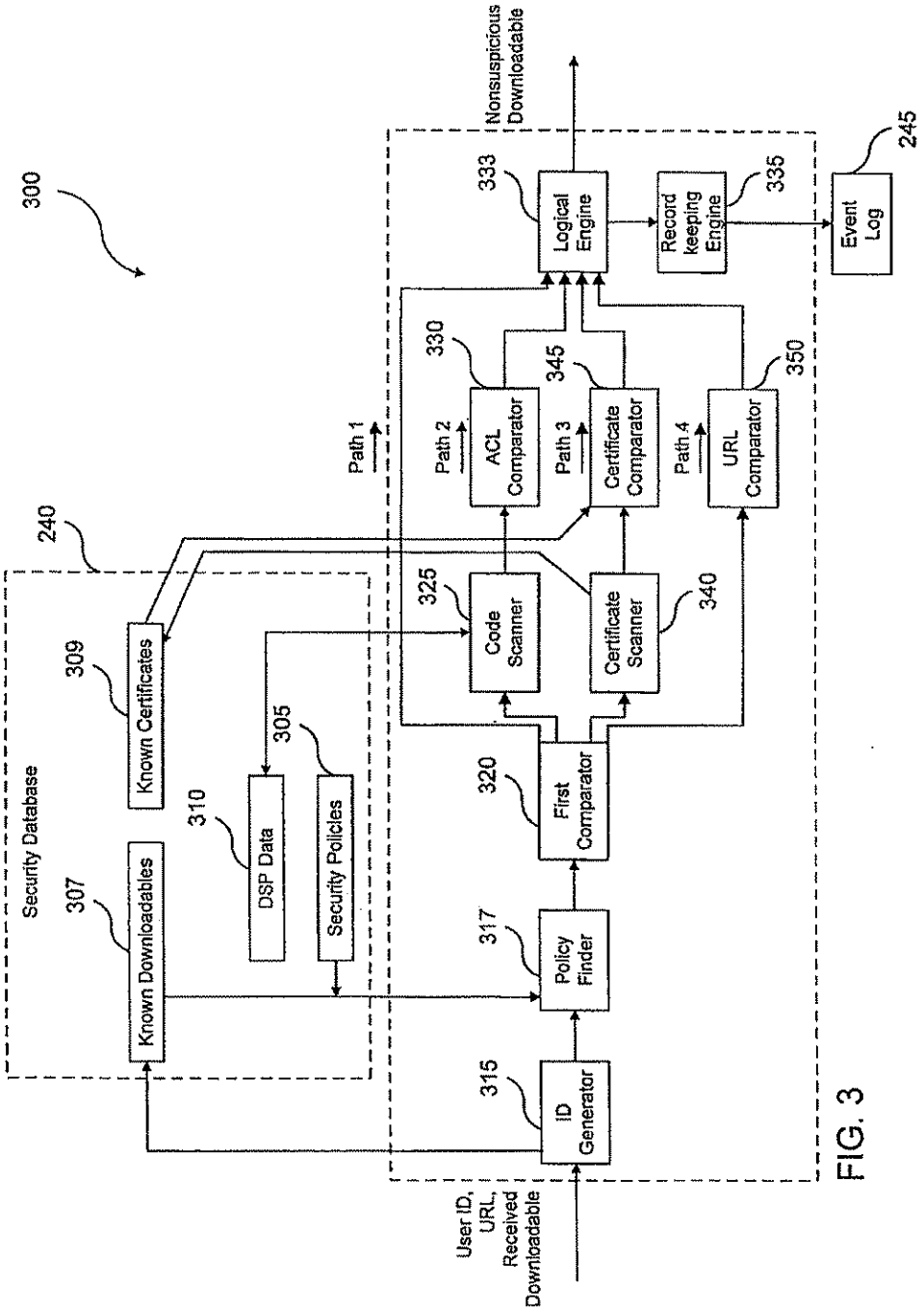

300
Nonsuspicious Downloadable
333
Logical Engine
Record keeping Engine
335
Event Log
245
330
ACL Comparator
345
Certificate Comparator
350
URL Comparator
Path 1
Path 2
Path 3
Path 4
240
325
Code Scanner
Certificate Scanner
340
309
Known Certificates
305
310
DSP Data
Security Policies
Security Database
307
Known Downloadables
320
First Comparator
317
Policy Finder
315
ID Generator
User ID, URL, Received Downloadable

FIG. 3

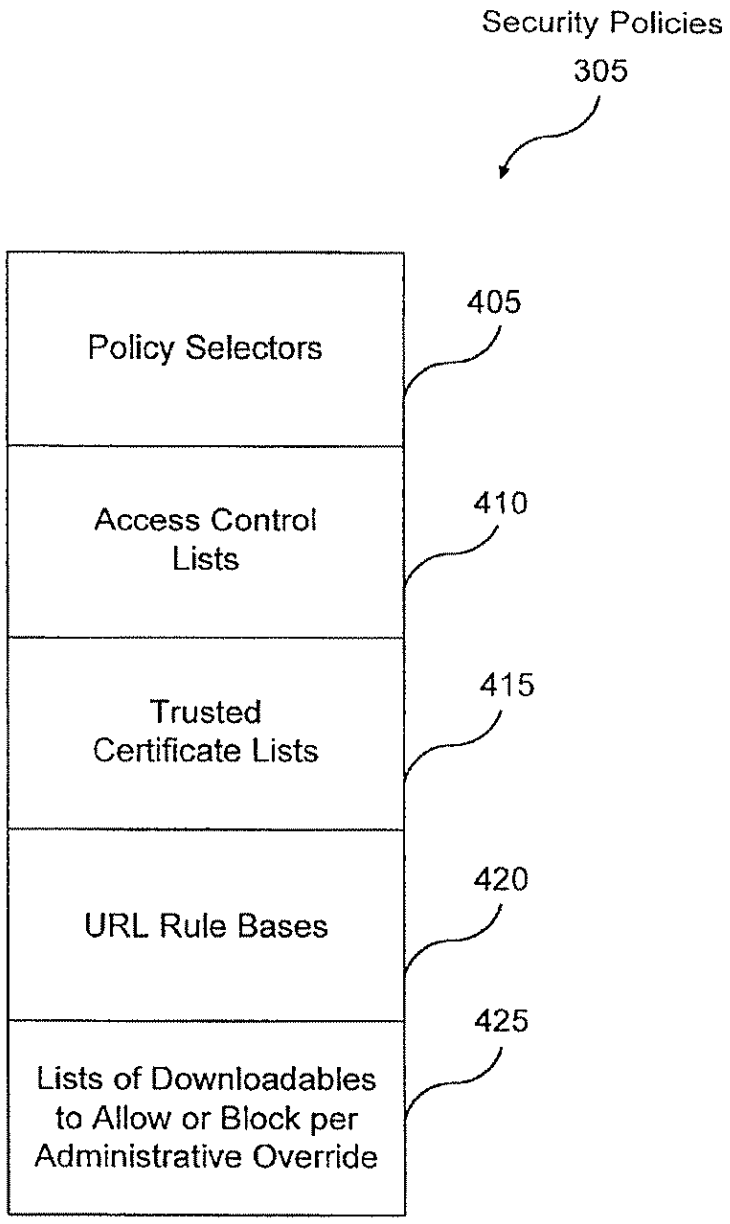

Security Policies
305
Policy Selectors
405
Access Control Lists
410
Trusted Certificate Lists
415
URL Rule Bases
420
Lists of Downloadables to Allow or Block per Administrative Override
425

FIG. 4

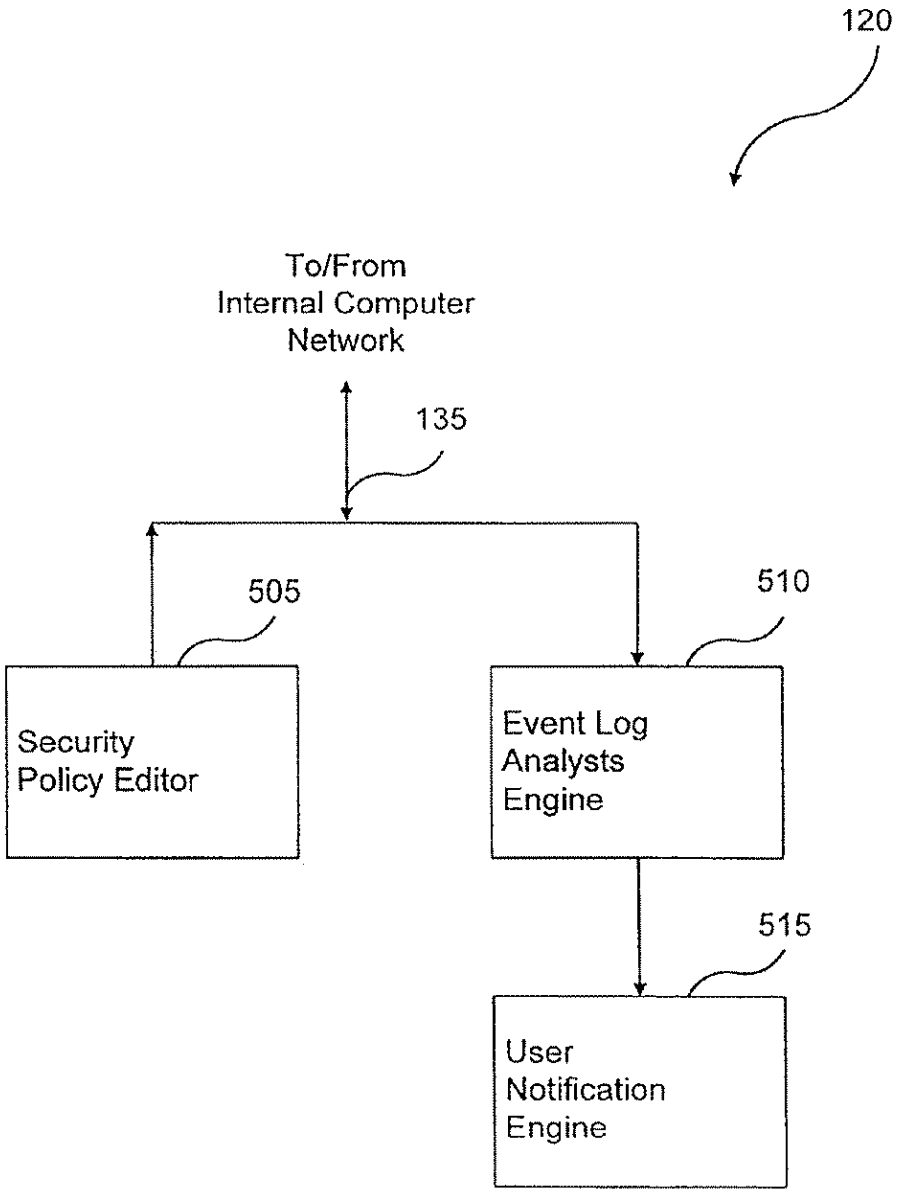

120
To/From
Internal Computer
Network
135
505
510
Security
Policy Editor
Event Log
Analysts
Engine
515
User
Notification
Engine

FIG. 5

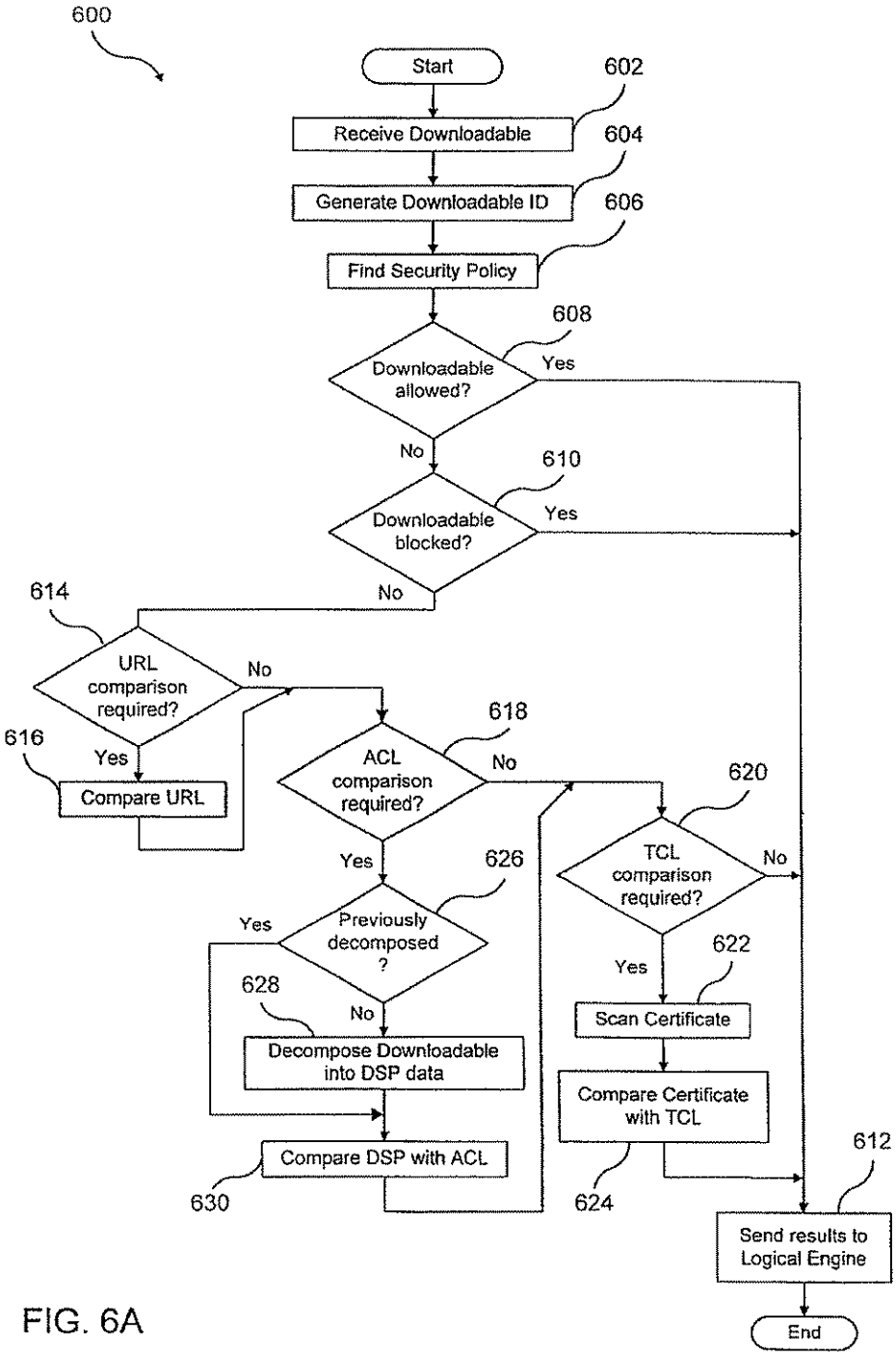

600
Start
602
Receive Downloadable
604
Generate Downloadable ID
606
Find Security Policy
608
Downloadable allowed?
Yes
No
610
Downloadable blocked?
Yes
No
614
URL comparison required?
No
616
Yes
Compare URL
618
ACL comparison required?
No
620
TCL comparison required?
No
Yes
626
Previously decomposed ?
Yes
628
No
Decompose Downloadable into DSP data
Compare DSP with ACL
630
Yes
622
Scan Certificate
Compare Certificate with TCL
624
612
Send results to Logical Engine
End

FIG. 6A

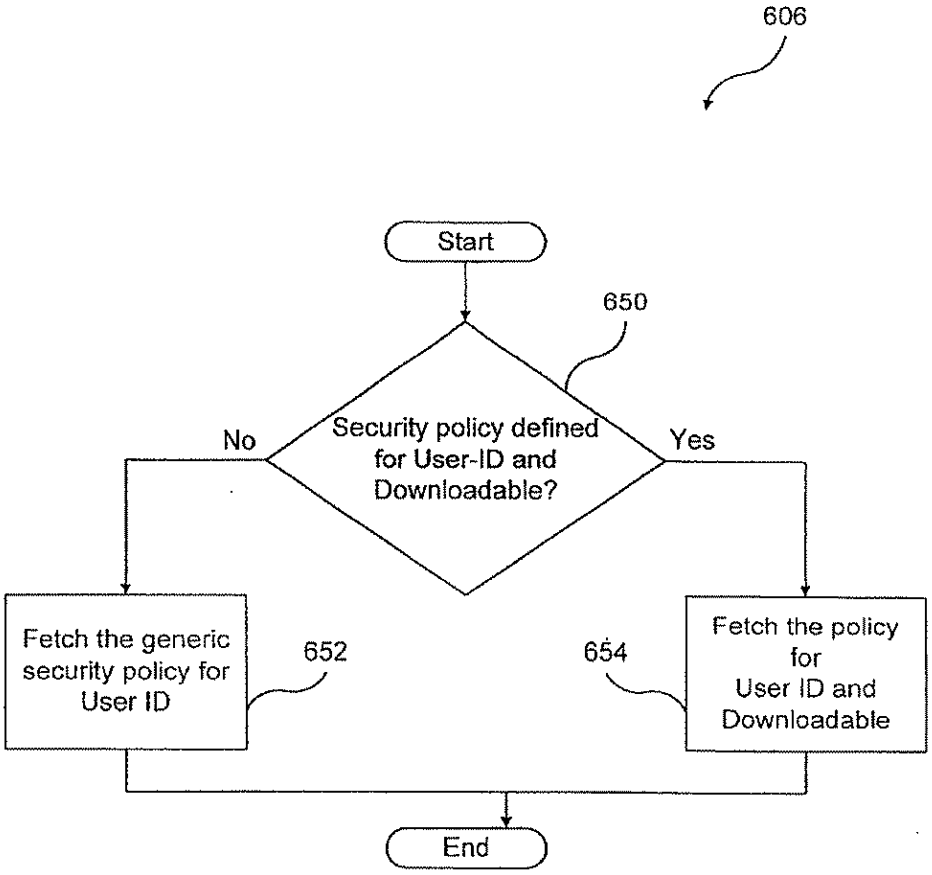

606
Start
650
Security policy defined for User-ID and Downloadable?
No
Yes
Fetch the generic security policy for User ID
652
654
Fetch the policy for User ID and Downloadable
End

FIG. 6B

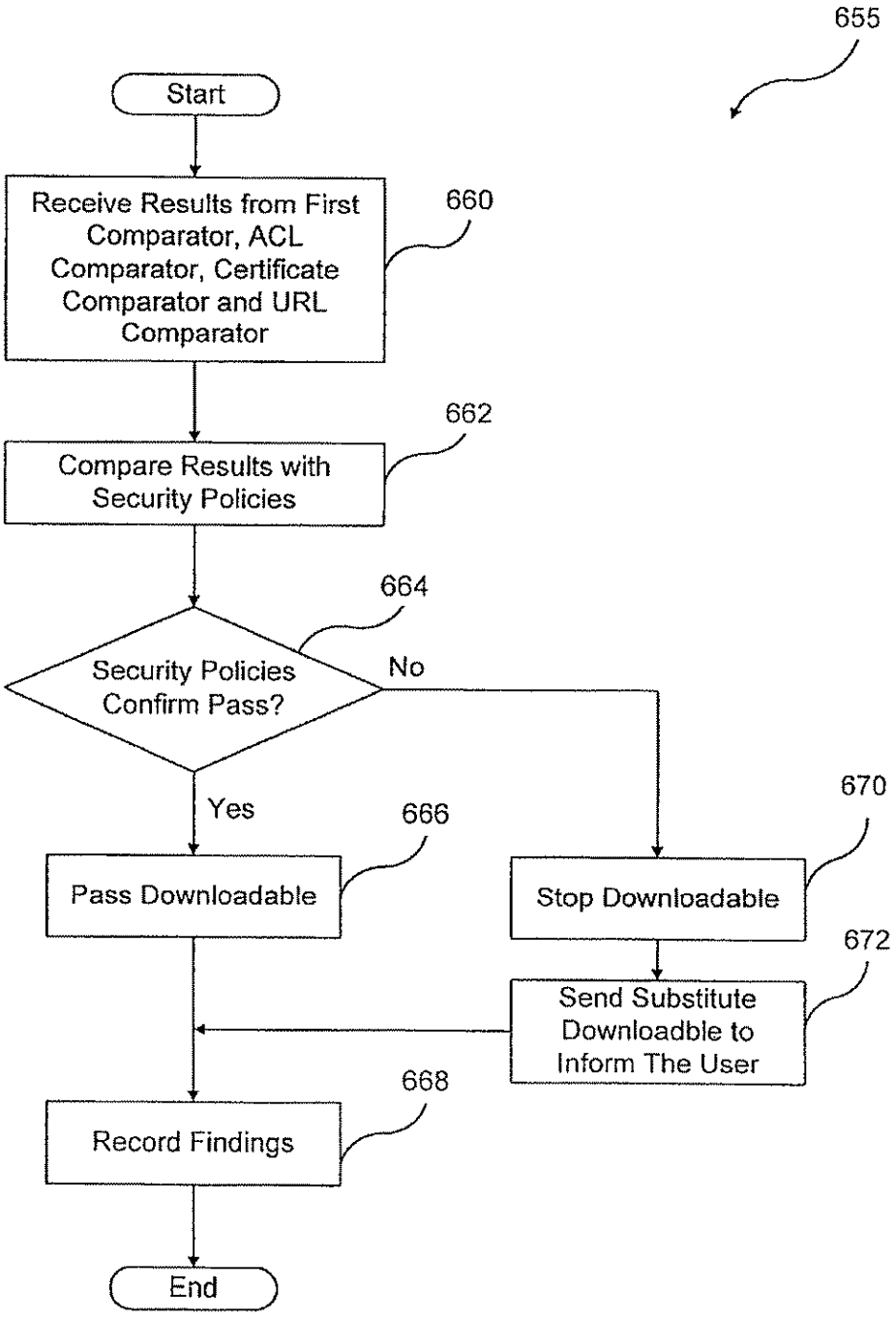

655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
Security Policies Confirm Pass?
664
No
Yes
Pass Downloadable
666
Stop Downloadable
670
Send Substitute Downloadble to Inform The User
672
Record Findings
668
End

FIG. 6C

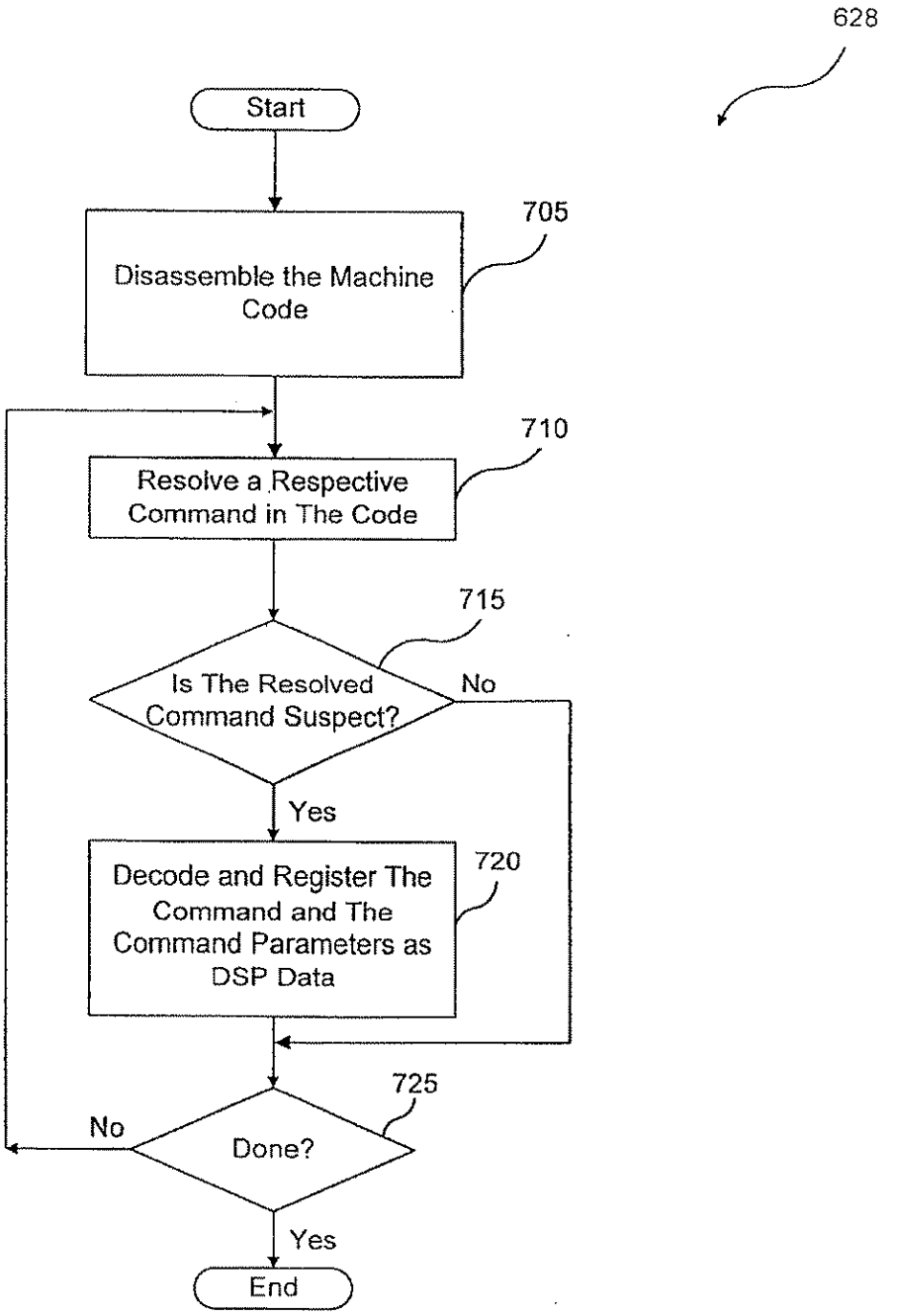

628
Start
705
Disassemble the Machine Code
710
Resolve a Respective Command in The Code
715
Is The Resolved Command Suspect?
No
Yes
720
Decode and Register The Command and The Command Parameters as DSP Data
725
Done?
No
Yes
End

FIG. 7

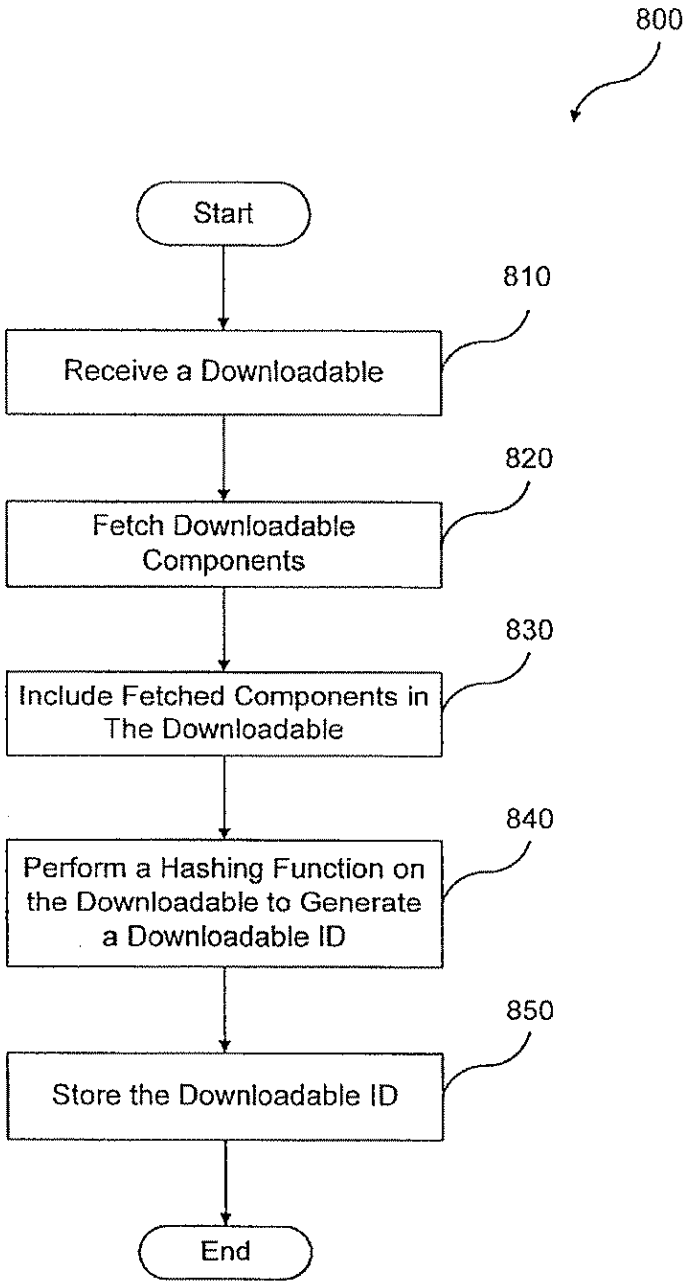

800
Start
810
Receive a Downloadable
820
Fetch Downloadable Components
830
Include Fetched Components in The Downloadable
840
Perform a Hashing Function on the Downloadable to Generate a Downloadable ID
850
Store the Downloadable ID
End

FIG. 8

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

PRIORITY REFERENCE TO RELATED APPLICATION

This application is a continuation of and hereby incorporates by reference U.S. patent application Ser. No. 08/964,388, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables," filed Nov. 6, 1997, which is now U.S. Pat. No. 6,092,194, which claims priority to provisional application Serial No. 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov. 8, 1996, by inventor Shlomo Touboul.

INCORPORATION BY REFERENCE TO RELATED APPLICATIONS

This application hereby incorporates by reference related U.S. patent application Ser. No. 08/790,097, entitled "System and Method for Protecting a Client from Hostile Downloadables," filed on Jan. 29, 1997, which is now U.S. Pat. No. 6,167,520, by inventor Shlomo Touboul; and hereby incorporates by reference provisional application Ser. No. 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov. 8, 1996, by inventor Shlomo Touboul.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and method for protecting a computer and a network from hostile Downloadables.

2. Description of the Background Art

The Internet is currently a collection of over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate. Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

Accordingly, programmers continue to design computer and computer network security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as "Downloadables." A Downloadable is an executable application program, which is downloaded from a source computer and run on the destination computer. Downloadable is typically requested by an ongoing process such as by an Internet browser or web engine. Examples of Downloadables include Java™ applets designed for use in the Java™ distributing environment developed by Sun Microsystems, Inc., JavaScript scripts also developed by Sun Microsystems, Inc., ActiveX™ controls designed for use in the ActiveX™ distributing environment developed by the Microsoft Corporation, and Visual Basic also developed by the Microsoft Corporation. Therefore, a system and method are needed to protect a network from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a network from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied based on the client/group and on the particular Downloadable received. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components.

Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

The present invention further provides a method for protecting a computer from suspicious Downloadables. The method comprises the steps of receiving a Downloadable, comparing the Downloadable against a security policy to determine if the security policy has been violated, and discarding the Downloadable if the security policy has been violated.

It will be appreciated that the system and method of the present invention may provide computer protection from known hostile Downloadables. The system and method of the present invention may identify Downloadables that perform operations deemed suspicious. The system and method of the present invention may examine the Downloadable code to determine whether the code contains any suspicious operations, and thus may allow or block the Downloadable accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a network system, in accordance with the present invention;

FIG. 2 is a block diagram illustrating details of the internal network security system of FIG. 1;

FIG. 3 is a block diagram illustrating details of the security program and the security database of FIG. 2;

FIG. 4 is a block diagram illustrating details of the security policies of FIG. 3;

FIG. 5 is a block diagram illustrating details of the security management console of FIG. 1;

FIG. 6A is a flowchart illustrating a method of examining for suspicious Downloadables, in accordance with the present invention;

FIG. 6B is a flowchart illustrating details of the step for finding the appropriate security policy of FIG. 6A;

FIG. 6C is a flowchart illustrating a method for determining whether an incoming Downloadable is to be deemed suspicious;

FIG. 7 is a flowchart illustrating details of the FIG. 6 step of decomposing a Downloadable; and

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a block diagram illustrating a network system **100**, in accordance with the present invention. The network system **100** includes an external computer network **105**, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a communications channel **125** to an internal network security system **110**. The network system **100** further includes an internal computer network **115**, such as a corporate Local Area Network (LAN), coupled via a communications channel **130** to the internal network computer system **110** and coupled via a communications channel **135** to a security management console **120**.

The internal network security system **110** examines Downloadables received from external computer network **105**, and prevents Downloadables deemed suspicious from reaching the internal computer network **115**. It will be further appreciated that a Downloadable is deemed suspicious if it performs or may perform any undesirable operation, or if it threatens or may threaten the integrity of an internal computer network **115** component. It is to be understood that the term "suspicious" includes hostile, potentially hostile, undesirable, potentially undesirable, etc. Security management console **120** enables viewing, modification and configuration of the internal network security system **110**.

FIG. **2** is a block diagram illustrating details of the internal network security system **110**, which includes a Central Processing Unit (CPU) **205**, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a signal bus **220**. The internal network security system **110** further includes an external communications interface **210** coupled between the communications channel **125** and the signal bus **220** for receiving Downloadables from external computer network **105**, and an internal communications interface **225** coupled between the signal bus **220** and the communications channel **130** for forwarding Downloadables not deemed suspicious to the internal computer network **115**. The external communications interface **210** and the internal communications interface **225** may be functional components of an integral communications interface (not shown) for both receiving Downloadables from the external computer network **105** and forwarding Downloadables to the internal computer network **115**.

Internal network security system **110** further includes Input/Output (I/O) interfaces **215** (such as a keyboard, mouse and Cathode Ray Tube (CRT) display), a data storage device **230** such as a magnetic disk, and a Random-Access Memory (RAM) **235**, each coupled to the signal bus **220**. The data storage device **230** stores a security database **240**, which includes security information for determining whether a received Downloadable is to be deemed suspicious. The data storage device **230** further stores a users list **260** identifying the users within the internal computer network **115** who may receive Downloadables, and an event log **245** which includes determination results for each Downloadable examined and runtime indications of the internal network security system **110**. An operating system **250** controls processing by CPU **205**, and is typically stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution. A security program **255** controls examination of incoming Downloadables, and also may be stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution by CPU **205**.

FIG. **3** is a block diagram illustrating details of the security program **255** and the security database **240**. The security program **255** includes an ID generator **315**, a policy finder **317** coupled to the ID generator **315**, and a first comparator **320** coupled to the policy finder **317**. The first comparator **320** is coupled to a logical engine **333** via four separate paths, namely, via Path **1**, via Path **2**, via Path **3** and via Path **4**. Path **1** includes a direct connection from the first comparator **320** to the logical engine **333**. Path **2** includes a code scanner coupled to the first comparator **320**, and an Access Control List (ACL) comparator **330** coupling the code scanner **325** to the logical engine **333**. Path **3** includes a certificate scanner **340** coupled to the first comparator **320**, and a certificate comparator **345** coupling the certificate scanner **340** to the logical engine **333**. Path **4** includes a Uniform Resource Locator (URL) comparator **350** coupling the first comparator **320** to the logical engine **3330**. A record-keeping engine **335** is coupled between the logical engine **333** and the event log **245**.

The security program **255** operates in conjunction with the security database **240**, which includes security policies **305**, known Downloadables **307**, known Certificates **309** and Downloadable Security Profile (DSP) data **310** corresponding to the known Downloadables **307**. Security policies **305** includes policies specific to particular users **260** and default (or generic) policies for determining whether to allow or block an incoming Downloadable. These security policies **305** may identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable. Referring to FIG. **4**, security policies **305** include policy selectors **405**, access control lists **410**, trusted certificate lists **415**, URL rule bases **420**, and lists **425** of Downloadables to allow or to block per administrative override.

Known Downloadables **307** include lists of Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, of Downloadables which OEMs know to be non-hostile, and of Downloadables previously received by this security program **255**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by each known Downloadable **307**, and may also include the respective arguments of these operations. An identified argument of an operation is referred to as "resolved." An unidentified argument is referred to as "unresolved." DSP data **310** is described below with reference to the code scanner **325**.

The ID generator **315** receives a Downloadable (including the URL from which it came and the userID of the intended recipient) from the external computer network **105** via the external communications interface **210**, and generates a Downloadable ID for identifying each Downloadable. The Downloadable ID preferably includes a digital hash of the complete Downloadable code. The ID generator **315** preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator **315** may prefetch all classes embodied in or identified by the Java™ applet bytecode to generate the Downloadable ID. Similarly, the ID generator **315** may retrieve all components listed in the INF file for an ActiveX™ control to compute a Downloadable ID. Accordingly, the Downloadable ID for the Downloadable will be the same each time the ID generator **315** receives the same Downloadable. The ID generator **315** adds the generated Downloadable ID to the list of known Downloadables

307 (if it is not already listed). The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317.

The policy finder 317 uses the userID of the intended user and the Downloadable ID to select the specific security policy 305 that shall be applied on the received Downloadable. If there is a specific policy 305 that was defined for the user (or for one of its super groups) and the Downloadable, then the policy is selected. Otherwise the generic policy 305 that was defined for the user (or for one of its super groups) is selected. The policy finder 317 then sends the policy to the first comparator 320.

The first comparator 320 receives the Downloadable, the Downloadable ID and the security policy 305 from the policy finder 317. The first comparator 320 examines the security policy 305 to determine which steps are needed for allowing the Downloadable. For example, the security policy 305 may indicate that, in order to allow this Downloadable, it must pass all four paths, Path 1, Path 2, Path 3 and Path 4. Alternatively, the security policy 305 may indicate that to allow the Downloadable, the it must pass only one of the paths. The first comparator 320 responds by forwarding the proper information to the paths identified by the security policy 305.

Path 1

In path 1, the first comparator 320 checks the policy selector 405 of the security policy 305 that was received from the policy finder 317. If the policy selector 405 is either "Allowed" or "Blocked," then the first comparator 320 forwards this result directly to the logical engine 333. Otherwise, the first comparator 320 invokes the comparisons in path2 and/or path 3 and/or path 4 based on the contents of policy selector 405. It will be appreciated that the first comparator 320 itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override 425. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked."

Alternatively, the logical engine 333 may receive the results of each of the paths and based on the policy selector 405 may institute the final determination whether to allow or block the Downloadable. The first comparator 320 informs the logical engine 333 of the results of its comparison.

Path 2

In path 2, the first comparator 320 delivers the Downloadable, the Downloadable ID and the security policy 305 to the code scanner 325. If the DSP data 310 of the received Downloadable is known, the code scanner 325 retrieves and forwards the information to the ACL comparator 330. Otherwise, the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker.

An Example List of Operations Deemed Potentially Hostile

File operations: READ a file, WRITE a file;

Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET;

Registry operations: READ a registry item, WRITE a registry item;

Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAD, KILL PROCESS/THREAD, CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc.; and

Resource usage thresholds: memory, CPU, graphics, etc.

In the preferred embodiment, the code scanner 325 performs a full-content inspection. However, for improved speed but reduced security, the code scanner 325 may examine only a portion of the Downloadable such as the Downloadable header. The code scanner 325 then stores the DSP data into DSP data 310 (corresponding to its Downloadable ID), and sends the Downloadable, the DSP data to the ACL comparator 330 for comparison with the security policy 305.

The ACL comparator 330 receives the Downloadable, the corresponding DSP data and the security policy 305 from the code scanner 325, and compares the DSP data against the security policy 305. That is, the ACL comparator 330 compares the DSP data of the received Downloadable against the access control lists 410 in the received security policy 305. The access control list 410 contains criteria indicating whether to pass or fail the Downloadable. For example, an access control list may indicate that the Downloadable fails if the DSP data includes a WRITE command to a system file. The ACL comparator 330 sends its results to the logical engine 333.

Path 3

In path 3, the certificate scanner 340 determines whether the received Downloadable was signed by a certificate authority, such as VeriSign, Inc., and scans for a certificate embodied in the Downloadable. The certificate scanner 340 forwards the found certificate to the certificate comparator 345. The certificate comparator 345 retrieves known certificates 309 that were deemed trustworthy by the security administrator and compares the found certificate with the known certificates 309 to determine whether the Downloadable was signed by a trusted certificate. The certificate comparator 345 sends the results to the logical engine 333.

Path 4

In path 4, the URL comparator 350 examines the URL identifying the source of the Downloadable against URLs stored in the URL rule base 420 to determine whether the Downloadable comes from a trusted source. Based on the security policy 305, the URL comparator 350 may deem the Downloadable suspicious if the Downloadable comes from an untrustworthy source or if the Downloadable did not come from a trusted source. For example, if the Downloadable comes from a known hacker, then the Downloadable may be deemed suspicious and presumed hostile. The URL comparator 350 sends its results to the logical engine 333.

The logical engine 333 examines the results of each of the paths and the policy selector 405 in the security policy 305 to determine whether to allow or block the Downloadable. The policy selector 405 includes a logical expression of the results received from each of the paths. For example, the

logical engine **333** may block a Downloadable if it fails any one of the paths, i.e., if the Downloadable is known hostile (Path **1**), if the Downloadable may request suspicious operations (Path **2**), if the Downloadable was not signed by a trusted certificate authority (Path **3**), or if the Downloadable did came from an untrustworthy source (Path **4**). The logical engine **333** may apply other logical expressions according to the policy selector **405** embodied in the security policy **305**. If the policy selector **405** indicates that the Downloadable may pass, then the logical engine **333** passes the Downloadable to its intended recipient. Otherwise, if the policy selector **405** indicates that the Downloadable should be blocked, then the logical engine **333** forwards a non-hostile Downloadable to the intended recipient to inform the user that internal network security system **110** discarded the original Downloadable. Further, the logical engine **333** forwards a status report to the record-keeping engine **335**, which stores the reports in event log **245** in the data storage device **230** for subsequent review, for example, by the MIS director.

FIG. **5** is a block diagram illustrating details of the security management console **120**, which includes a security policy editor **505** coupled to the communications channel **135**, an event log analysis engine **510** coupled between communications channel **135** and a user notification engine **515**, and a Downloadable database review engine **520** coupled to the communications channel **135**. The security management console **120** further includes computer components similar to the computer components illustrated in FIG. **2**.

The security policy editor **505** uses an I/O interface similar to I/O interface **215** for enabling authorized user modification of the security policies **305**. That is, the security policy editor **505** enables the authorized user to modify specific security policies **305** corresponding to the users **260**, the default or generic security policy **305**, the Downloadables to block per administrative override, the Downloadables to allow per administrative override, the trusted certificate lists **415**, the policy selectors **405**, the access control lists **410**, the URLs in the URL rule bases **420**, etc. For example, if the authorized user learns of a new hostile Downloadable, then the user can add the Downloadable to the Downloadables to block per system override.

The event log analysis engine **510** examines the status reports contained in the event log **245** stored in the data storage device **230**. The event log analysis engine **510** determines whether notification of the user (e.g., the security system manager or MIS director) is warranted. For example, the event log analysis engine **510** may warrant user notification whenever ten (10) suspicious Downloadables have been discarded by internal network security system **110** within a thirty (30) minute period, thereby flagging a potential imminent security threat. Accordingly, the event log analysis engine **510** instructs the user notification engine **515** to inform the user. The user notification engine **515** may send an e-mail via internal communications interface **220** or via external communications interface **210** to the user, or may display a message on the user's display device (not shown).

FIG. **6A** is a flowchart illustrating a method **600** for protecting an internal computer network **115** from suspicious Downloadables. Method **600** begins with the ID generator **315** in step **602** receiving a Downloadable. The ID generator **315** in step **604** generates a Downloadable ID identifying the received Downloadable, preferably, by generating a digital hash of the Downloadable code (including prefetched components). The policy finder **317** in step **606** finds the appropriate security policy **305** corresponding to the userID specifying intended recipient (or the group to which the intended recipient belongs) and the Downloadable. The selected security policy **305** may be the default security policy **305**. Step **606** is described in greater detail below with reference to FIG. **6B**.

The first comparator **320** in step **608** examines the lists of Downloadables to allow or to block per administrative override **425** against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically. If so, then in step **612** the first comparator **320** sends the results to the logical engine **333**. If not, then the method **600** proceeds to step **610**. In step **610**, the first comparator **620** examines the lists of Downloadables to block per administrative override **425** against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically. If so, then the first comparator **420** in step **612** sends the results to the logical engine **333**. Otherwise, method **600** proceeds to step **614**.

In step **614**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path **4**. If not, then method **600** jumps to step **618**. If so, then the URL comparator **350** in step **616** compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases **420**, and then method **600** proceeds to step **618**.

In step **618**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path **2**. If not, then method **600** jumps to step **620**. Otherwise, the code scanner **235** in step **626** examines the DSP data **310** based on the Downloadable ID of the incoming Downloadable to determine whether the Downloadable has been previously decomposed. If so, then method **600** jumps to step **630**. Otherwise, the code scanner **325** in step **628** decomposes the Downloadable into DSP data. Downloadable decomposition is described in greater detail with reference to FIG. **7**. In step **630**, the ACL comparator **330** compares the DSP data of the incoming Downloadable against the access control lists **410** (which include the criteria necessary for the Downloadable to fail or pass the test).

In step **620**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path **3**. If not, then method **600** returns to step **612** to send the results of each of the test performed to the logical engine **333**. Otherwise, the certificate scanner **622** in step **622** scans the Downloadable for an embodied certificate. The certificate comparator **345** in step **624** retrieves trusted certificates from the trusted certificate lists (TCL) **415** and compares the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source. Method **600** then proceeds to step **612** by the certificate scanner **345** sending the results of each of the paths taken to the logical engine **333**. The operations of the logical engine **333** are described in greater detail below with reference to FIG. **6C**. Method **600** then ends.

One skilled in the art will recognize that the tests may be performed in a different order, and that each of the tests need not be performed. Further, one skilled in the art will recognize that, although path **1** is described in FIG. **6A** as an automatic allowance or blocking, the results of Path **1** may be another predicate to be applied by the logical engine **333**. Further, although the tests are shown serially in FIG. **6A**, the tests may be performed in parallel as illustrated in FIG. **3**.

FIG. 6B is a flowchart illustrating details of step **606** of FIG. 6A (referred to herein as method **606**). Method **606** begins with the policy finder **317** in step **650** determining whether security policies **305** include a specific security policy corresponding to the userID and the Downloadable. If so, then the policy finder **317** in step **654** fetches the corresponding specific policy **305**. If not, then the policy finder **317** in step **652** fetches the default or generic security policy **305** corresponding to the userID. Method **606** then ends.

FIG. 6C is a flowchart illustrating details of a method **655** for determining whether to allow or to block the incoming Downloadable. Method **655** begins with the logical engine **333** in step **660** receiving the results from the first comparator **320**, from the ACL comparator **330**, from the certificate comparator **345** and from the URL comparator **350**. The logical engine **333** in step **662** compares the results with the policy selector **405** embodied in the security policy **305**, and in step **664** determines whether the policy selector **405** confirms the pass. For example, the policy selector **405** may indicate that the logical engine **333** pass the Downloadable if it passes one of the tests of Path **1**, Path **2**, Path **3** and Path **4**. If the policy selector **405** indicates that the Downloadable should pass, then the logical engine **333** in step **666** passes the Downloadable to the intended recipient. In step **668**, the logical engine **333** sends the results to the record-keeping engine **335**, which in turn stores the results in the event log **245** for future review. Method **655** then ends. Otherwise, if the policy selector **405** in step **664** indicates that the Downloadable should not pass, then the logical engine **333** in step **670** stops the Downloadable and in step **672** sends a non-hostile substitute Downloadable to inform the user that the incoming Downloadable has been blocked. Method **655** then jumps to step **668**.

FIG. **7** is a flowchart illustrating details of step **628** of FIG. **6A** (referred to herein as method **628**) for decomposing a Downloadable into DSP data **310**. Method **628** begins in step **705** with the code scanner **325** disassembling the machine code of the Downloadable. The code scanner **325** in step **710** resolves a respective command in the machine code, and in step **715** determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. **3**). If not, then the code scanner **325** in step **725** determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method **628** ends. Otherwise, method **628** returns to step **710**.

Otherwise, if the code scanner **325** in step **71** determines that the resolved command is suspect, then the code scanner **325** in step **720** decodes and registers the suspicious command and its command parameters as DSP data **310**. The code scanner **325** in step **720** registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method **628** then jumps to step **725**.

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable. Method **800** begins with the ID generator **315** in step **810** receiving a Downloadable from the external computer network **105**. The ID generator **315** in step **820** may fetch some or all components referenced in the Downloadable code, and in step **830** includes the fetched components in the Downloadable code. The ID generator **315** in step **840** performs a hashing function on at least a portion of the Downloadable code to generate a Downloadable ID. The ID generator **315** in step **850** stores the generated Downloadable ID in the security database **240** as a reference to the DSP data **310**. Accordingly, the Downloadable ID will be the same for the identical Downloadable each time it is encountered.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more references; and

performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

2. The method of claim **1**, wherein the Downloadable includes an applet.

3. The method of claim **1**, wherein the Downloadable includes an active software control.

4. The method of claim **1**, wherein the Downloadable includes a plugin.

5. The method of claim **1**, wherein the Downloadable includes HTML code.

6. The method of claim **1**, wherein the Downloadable includes an application program.

7. The method of claim **1**, wherein said fetching includes fetching a first software component referenced by the Downloadable.

8. The method of claim **1**, wherein said fetching includes fetching all software components referenced by the Downloadable.

9. A system for generating a Downloadable ID to identify a Downloadable, comprising:

a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and

an ID generator coupled to the communications engine that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

10. The system of claim **9**, wherein the Downloadable includes an applet.

11. The system of claim **9**, wherein the Downloadable includes an active software control.

12. The system of claim **9**, wherein the Downloadable includes a plugin.

13. The system of claim **9**, wherein the Downloadable includes HTML code.

14. The system of claim 9, wherein the Downloadable includes an application program.

15. The system of claim 9, wherein the ID generator fetches a first software component referenced by the Downloadable.

16. The method of claim 9, wherein the ID generator fetches all software components referenced by the Downloadable.

17. A system for generating a Downloadable ID to identify a Downloadable, comprising:

means for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

means for fetching at least one software component identified by the one or more references; and

means for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

18. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more references; and

performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

* * * * *

EXHIBIT C

US007058822B2

(12) **United States Patent**
Edery et al.

(10) **Patent No.: US 7,058,822 B2**
(45) **Date of Patent: Jun. 6, 2006**

(54) **MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS**

(75) Inventors: **Yigal Mordechai Edery**, Pardesia (IL); **Nimrod Itzhak Vered**, Goosh Tel-Mond (IL); **David R. Kroll**, San Jose, CA (US)

(73) Assignee: **Finjan Software, Ltd.**, South Netanya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1013 days.

(21) Appl. No.: **09/861,229**

(22) Filed: **May 17, 2001**

(65) **Prior Publication Data**

US 2002/0013910 A1 Jan. 31, 2002

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/551,302, filed on Apr. 18, 2000, now Pat. No. 6,480,962, which is a continuation-in-part of application No. 09/539,667, filed on Mar. 30, 2000, now Pat. No. 6,804,780.

(60) Provisional application No. 60/205,591, filed on May 17, 2000.

(51) **Int. Cl.**
G06F 11/30 (2006.01)

(52) **U.S. Cl.** **713/200**

(58) **Field of Classification Search** 713/176, 713/175, 200, 201, 150, 168; 701/223, 229; 717/120, 124, 126, 127, 130, 131, 134, 135; 709/223–229

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,077,677 A 12/1991 Murphy et al.
5,359,659 A 10/1994 Rosenthal
5,361,359 A 11/1994 Tajalli et al.
5,485,409 A 1/1996 Gupta et al.

(Continued)

OTHER PUBLICATIONS

Zhong et al, "Security in the large: is Java's sandbox scalable?", Oct. 1998, Seventh IEEE Symposium on Reliable Distributed Systems, pp 1-6.*

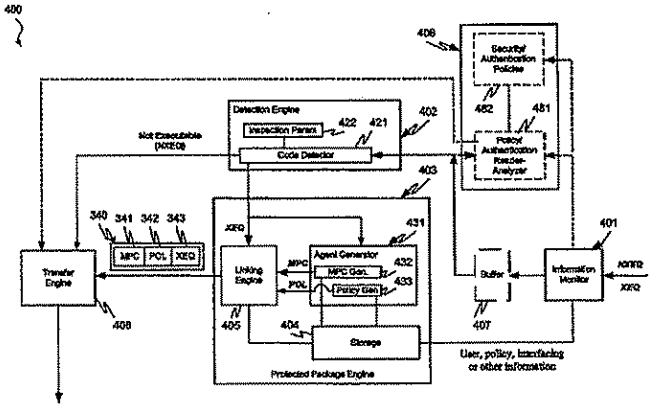
(Continued)

Primary Examiner—Christopher Revak
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey, L.L.P.

(57) **ABSTRACT**

Protection systems and methods provide for protecting one or more personal computers ("PCs") and/or other intermittently or persistently network accessible devices or processes from undesirable or otherwise malicious operations of Java™ applets, ActiveX™ controls, JavaScript™ scripts, Visual Basic scripts, add-ins, downloaded/uploaded programs or other "Downloadables" or "mobile code" in whole or part. A protection engine embodiment provides, within a server, firewall or other suitable "re-communicator," for monitoring information received by the communicator, determining whether received information does or is likely to include executable code, and if so, causes mobile protection code (MPC) to be transferred to and rendered operable within a destination device of the received information, more suitably by forming a protection agent including the MPC, protection policies and a detected-Downloadable. An MPC embodiment further provides, within a Downloadable-destination, for initiating the Downloadable, enabling malicious Downloadable operation attempts to be received by the MPC, and causing (predetermined) corresponding operations to be executed in response to the attempts, more suitably in conjunction with protection policies.

35 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

5,485,575	A	1/1996	Chess et al.	
5,572,643	A	11/1996	Judson	
5,606,668	A	2/1997	Shwed	
5,623,600	A	4/1997	Ji et al.	
5,638,446	A	6/1997	Rubin	
5,692,047	A	11/1997	McManis	
5,692,124	A	11/1997	Holden et al.	
5,720,033	A	2/1998	Deo	
5,724,425	A	3/1998	Chang et al.	
5,740,248	A	4/1998	Fieres et al.	
5,761,421	A	6/1998	van Hoff et al.	
5,765,205	A	6/1998	Breslau et al.	
5,784,459	A	7/1998	Devarakonda et al.	
5,796,952	A	8/1998	Davis et al.	
5,805,829	A	9/1998	Cohen et al.	
5,832,208	A	11/1998	Chen et al.	
5,850,559	A	12/1998	Angelo et al.	
5,859,966	A	1/1999	Hayman et al.	
5,864,683	A	1/1999	Boebert et al.	
5,892,904	A	4/1999	Atkinson et al.	
5,951,698	A	9/1999	Chen et al.	
5,956,481	A	9/1999	Walsh et al.	
5,974,549	A	10/1999	Golan	
5,978,484	A	11/1999	Apperson et al.	
5,983,348	A	11/1999	Ji	
6,092,194	A	7/2000	Touboul	
6,154,844	A	11/2000	Touboul et al.	
6,167,520	A	12/2000	Touboul	
6,425,058	B1	7/2002	Arimilli et al.	
6,434,668	B1	8/2002	Arimilli et al.	
6,434,669	B1	8/2002	Arimilli et al.	
6,480,962	B1	11/2002	Touboul	
6,519,679	B1	2/2003	Devireddy et al.	
6,732,179	B1 *	5/2004	Brown et al.	709/229

OTHER PUBLICATIONS

Rubin et al, "Mobile code security" Dec. 1998, IEEE Internet, pp 30-34.*

Schmid et al, "Protecting data from malicious software", 2002, Proceeding of the 18th Annual Computer Security Applications Conference, pp 1-10.*

Corradi et al, "A flexible access control service for Java mobile code", 2000, IEEE, pp 356-365.*

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990; pp. 21-29.

Okamoto, E. et al., "ID-Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013-5194, Jul. 19, 1990, Abstract and pp. 1169-1170. URL:http://iel.ihs.com:80/cgi-bin/iel_cgl?se...2ehts%26ViewTemplate%3ddocview%5fb%2ehts.

IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, Nov. 15, 1995, p. 6-7.

Norvin Leach et al, "IE 3.0 Applets Will Earn Certification", PC Week vol. 13, No. 29, Jul. 22, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software Ltd., Jul. 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996, including Abstract, Contents, Introduction and pp. 1-10.

"Finjan Announces a Personal Java™ Firewall For Web Browsers—the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, Oct. 21, 1996, 2 pages.

Company Profile "Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Articles published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Articles published on the Internet, 7 pages.

Mark LaDue, "Online Business Consultant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.

Ron Moritz, "Why We Shouldn't Fear Java." Java Report, Feb., 1997, pp. 51-56.

Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated Feb. 17, 1997, Printed Dec. 23, 1998. URL: http://www.microsoft.com/workshop/security/authcode/signfag.asp#9, pp. 1-13.

Zhang, X.N., "Secure Code Distrubtion", IEEE/IEE Electronic Library online, Computer, vol. 30, Issue 6, Jun., 1997, pp.: 76-79.

Khare, Rohit, "Microsoft Authenticode Analyzed", Jul. 22, 1996, 2 pages. URL: http://www.xent.com/FoRK-archive/summer96/0338.html.

"Release Notes for the Microsoft ActiveX Development Kit", Aug. 13, 1996, 11 pages URL: http://activex.adsp.or.jp/inetsdk/readme.txt.

"Microsoft ActiveX Software Development Kit", Aug. 12, 1996, 6 pages. URL: http://activex.adsp.or.jp/inetsdk/help.overview.htm.

* cited by examiner

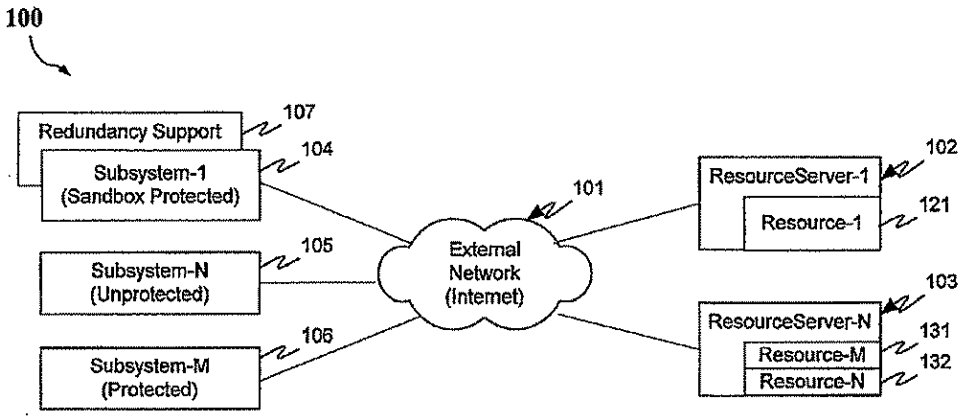


FIG. 1a

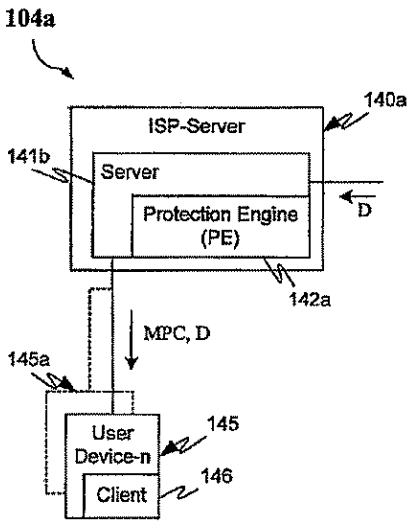


FIG. 1b

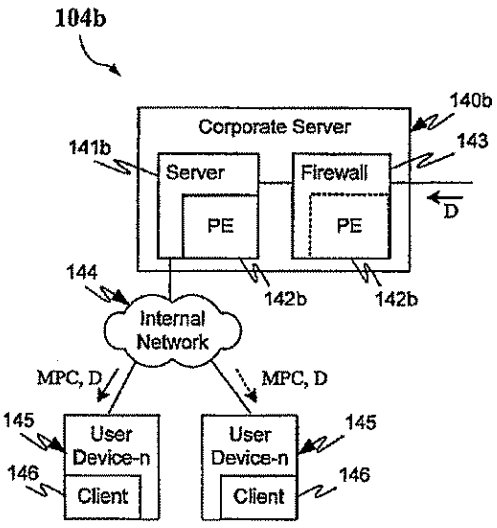


FIG. 1c

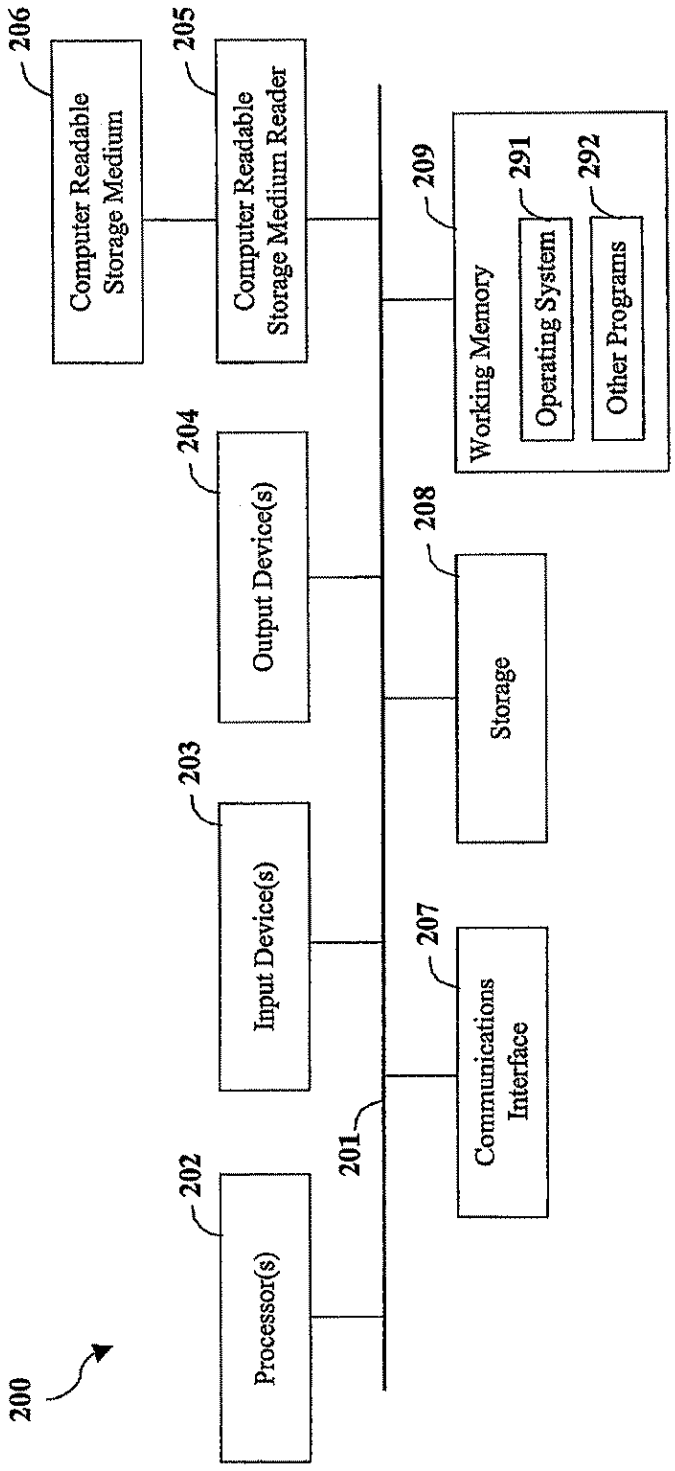

200
Processor(s)
202
Input Device(s)
203
Output Device(s)
204
Computer Readable Storage Medium
206
Computer Readable Storage Medium Reader
205
Communications Interface
207
Storage
208
Working Memory
209
Operating System
291
Other Programs
292
201

FIG. 2

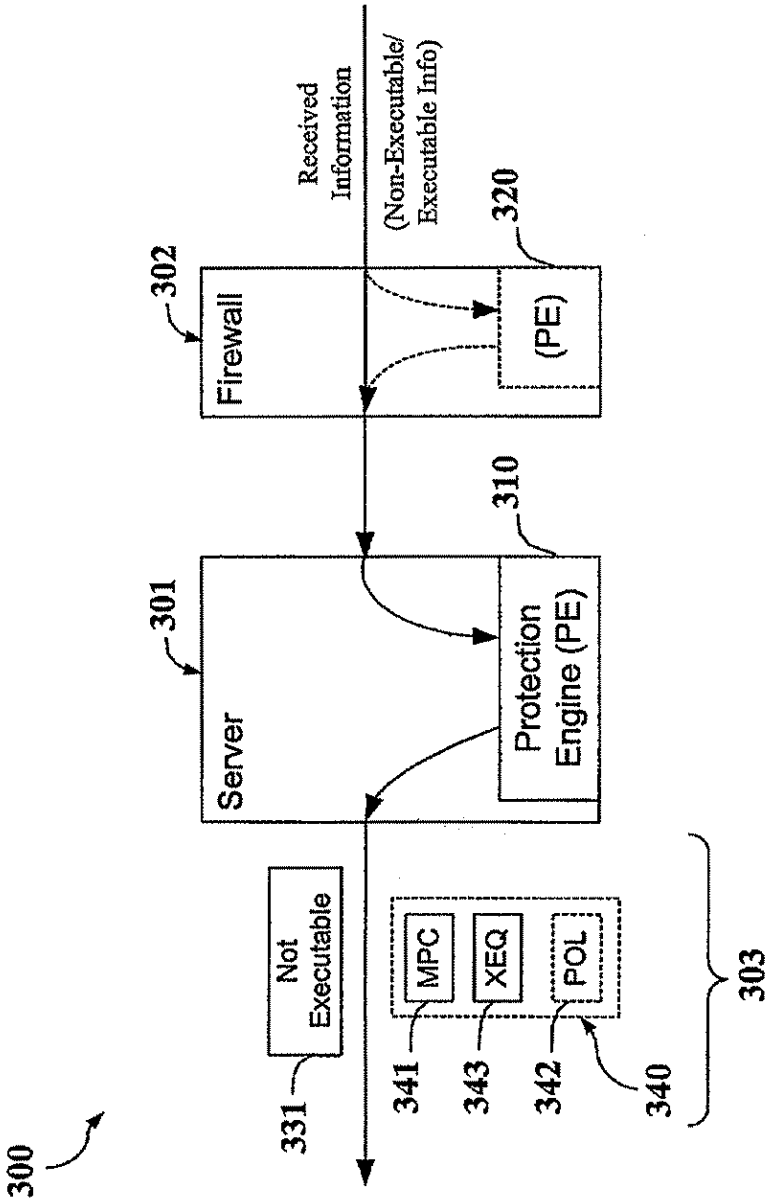

Received Information
(Non-Executable/ Executable Info)
320
302
Firewall
(PE)
310
301
Server
Protection Engine (PE)
Not Executable
MPC
XEQ
POL
303
341
343
342
340
331
300

FIG. 3

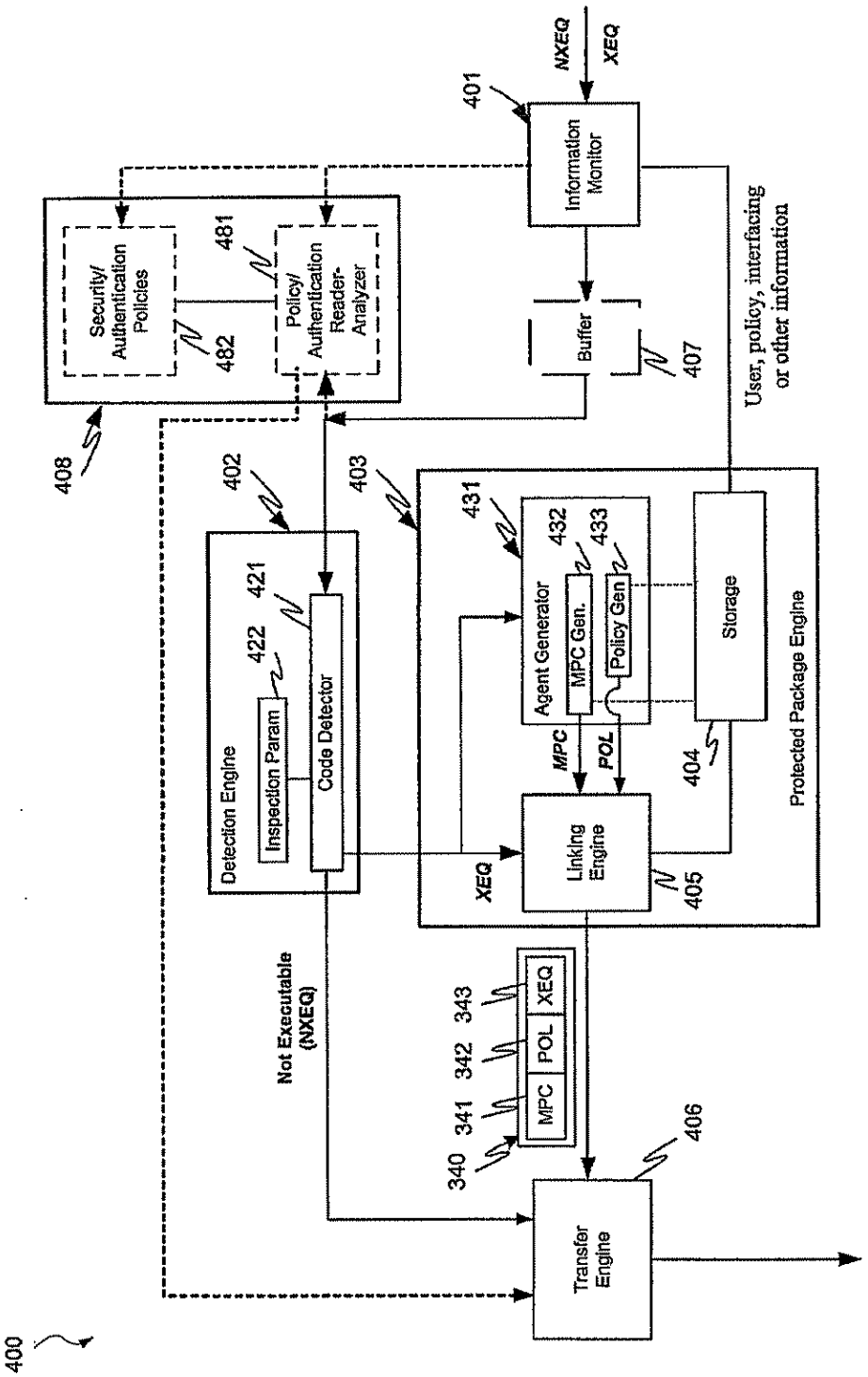

NXEQ
XEQ
401
Information Monitor
User, policy, interfacing or other information
Security/ Authentication Policies
481
Policy/ Authentication Reader-Analyzer
482
Buffer
407
408
402
403
431
Agent Generator
432
MPC Gen.
433
Policy Gen
Storage
Detection Engine
421
422
Inspection Param
Code Detector
MPC
POL
404
Protected Package Engine
XEQ
Linking Engine
405
Not Executable (NXEQ)
343
342
341
340
XEQ
POL
MPC
406
Transfer Engine
400

FIG. 4

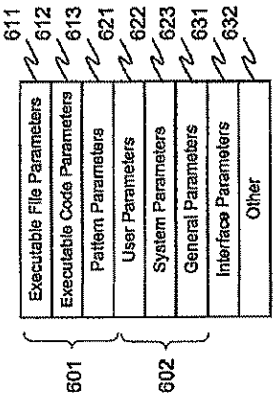


FIG. 6a

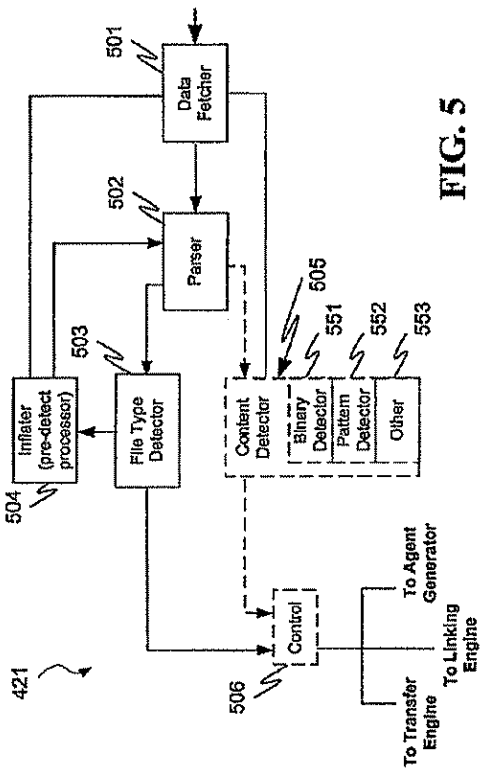


FIG. 5

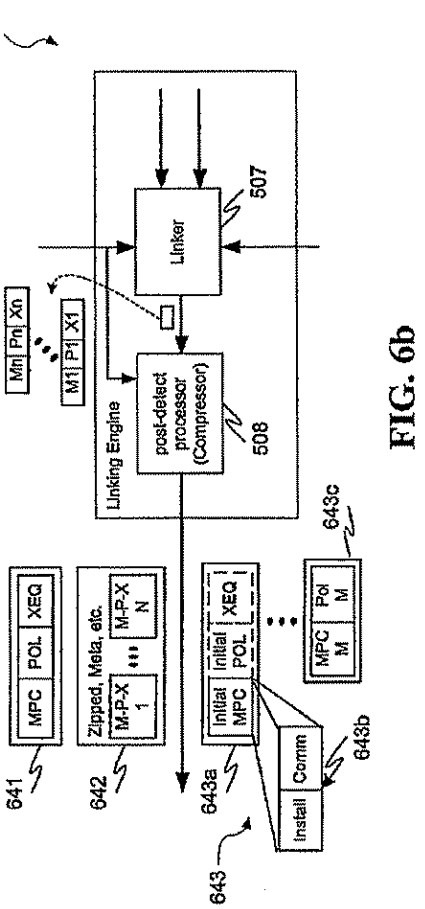


FIG. 6b

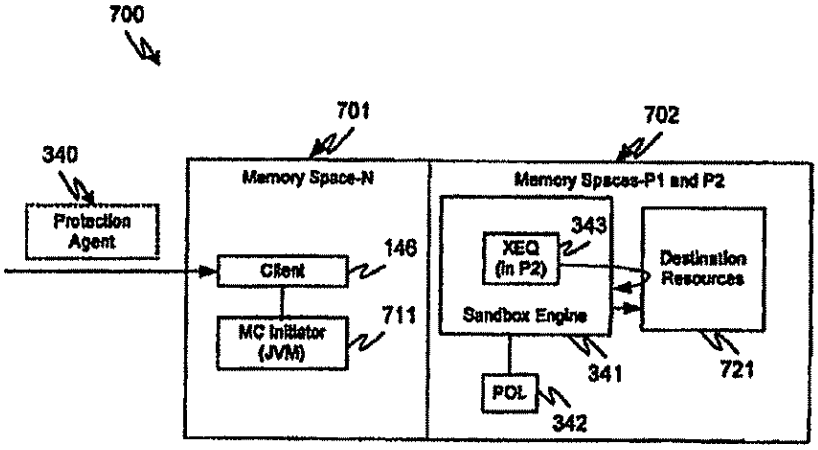


FIG. 7a

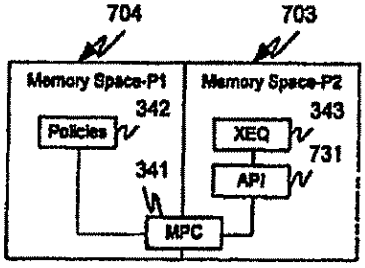


FIG. 7b

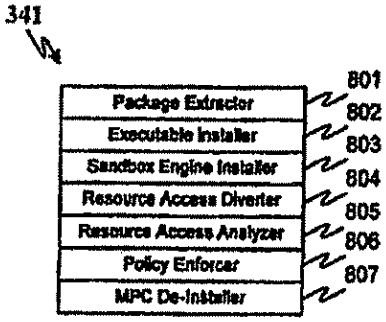


FIG. 8

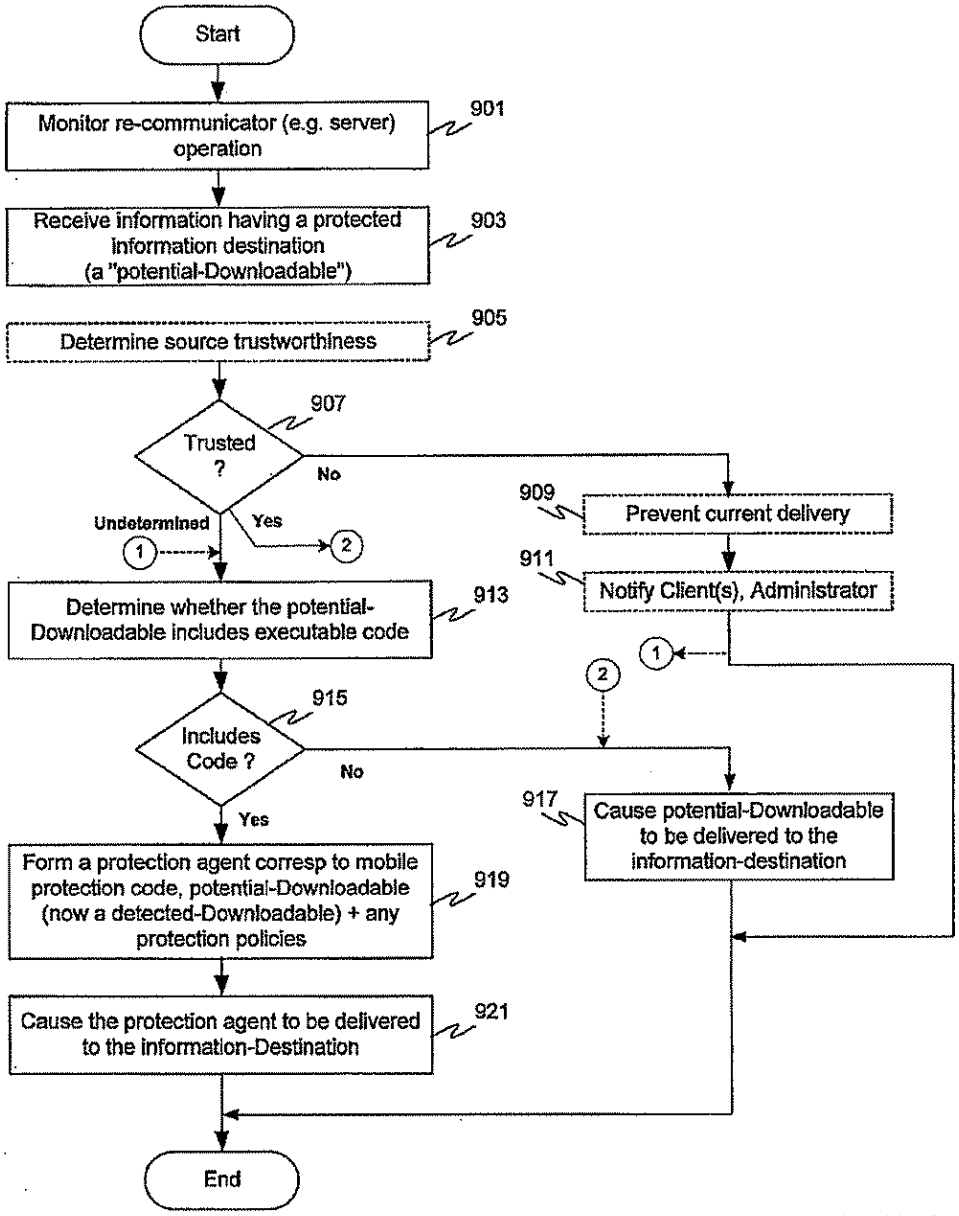

Start
Monitor re-communicator (e.g. server) operation
901
Receive information having a protected information destination (a "potential-Downloadable")
903
Determine source trustworthiness
905
Trusted ?
907
No
Undetermined
Yes
1
2
909
Prevent current delivery
911
Notify Client(s), Administrator
Determine whether the potential-Downloadable includes executable code
913
Includes Code ?
915
No
Yes
917
Cause potential-Downloadable to be delivered to the information-destination
Form a protection agent corresp to mobile protection code, potential-Downloadable (now a detected-Downloadable) + any protection policies
919
Cause the protection agent to be delivered to the information-Destination
921
End

FIG. 9

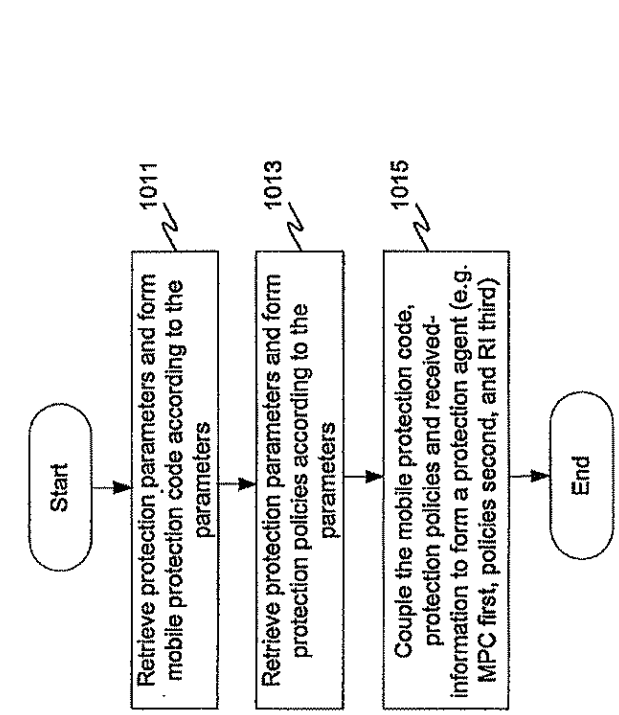


FIG. 10B

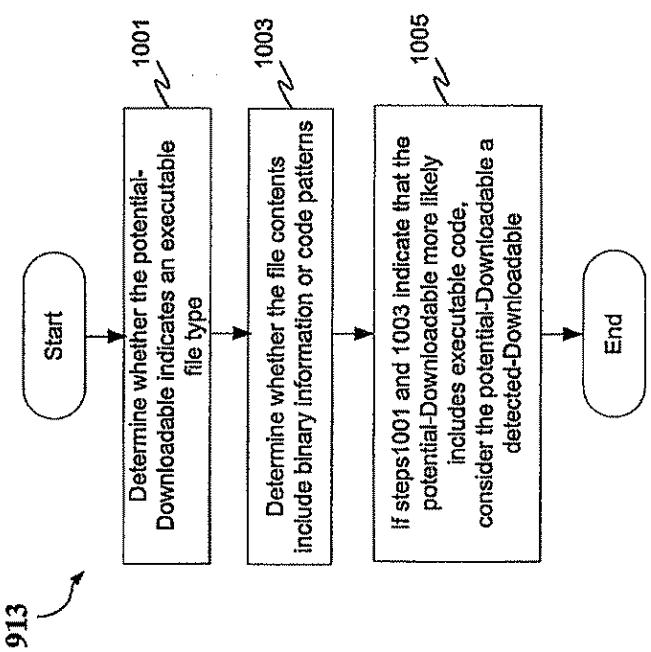


FIG. 10A

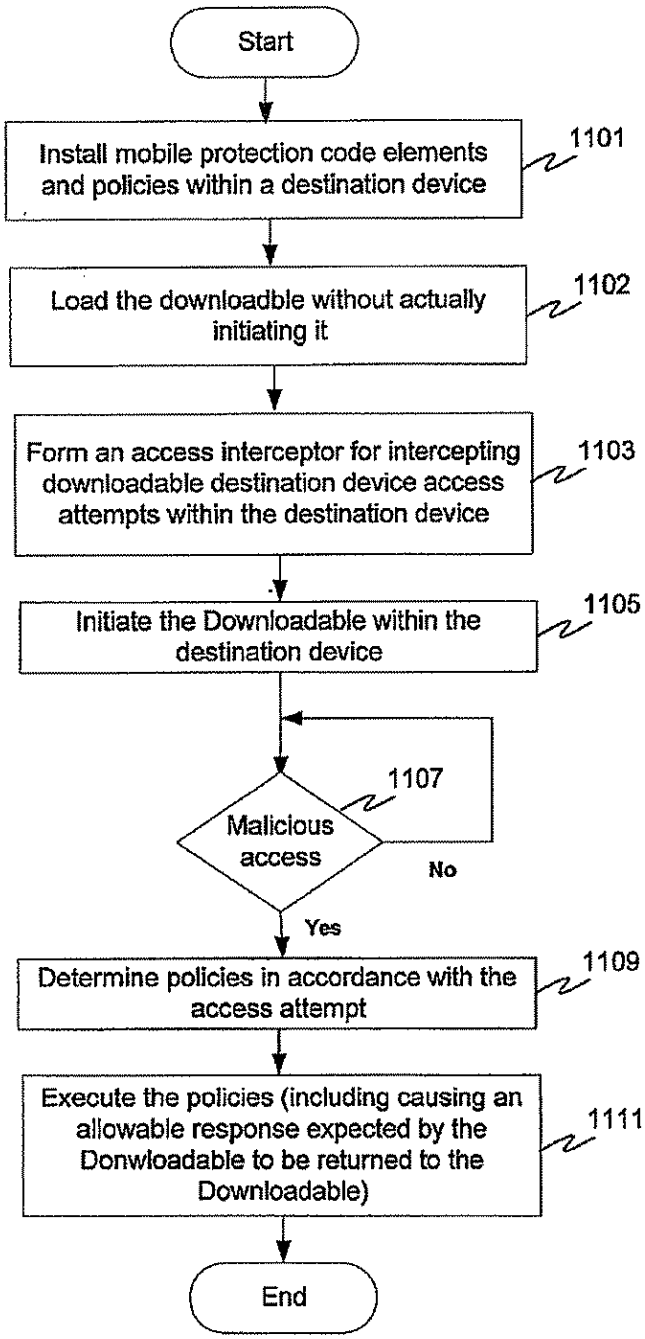

Start
Install mobile protection code elements and policies within a destination device
1101
Load the downloadble without actually initiating it
1102
Form an access interceptor for intercepting downloadable destination device access attempts within the destination device
1103
Initiate the Downloadable within the destination device
1105
Malicious access
1107
No
Yes
Determine policies in accordance with the access attempt
1109
Execute the policies (including causing an allowable response expected by the Donwloadable to be returned to the Downloadable)
1111
End

FIG. 11

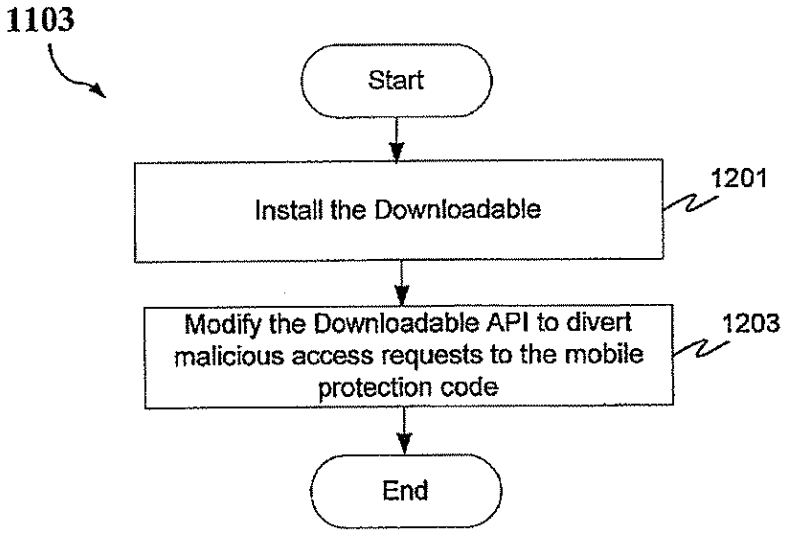


FIG. 12a

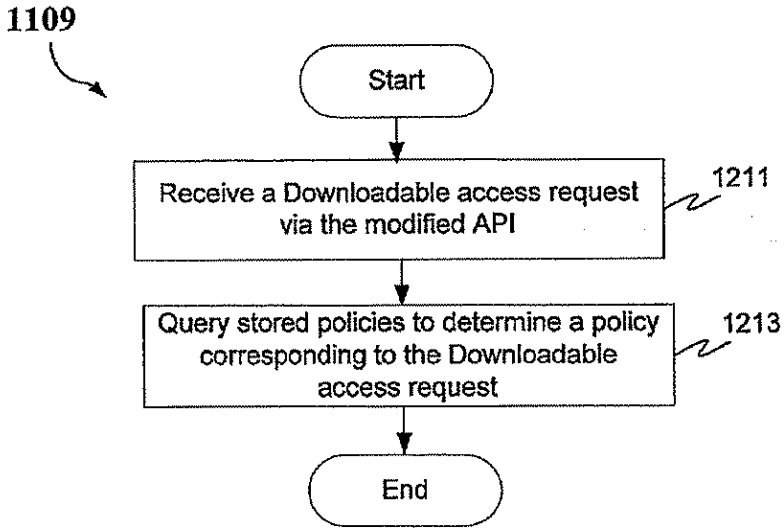


FIG. 12b

MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS

PRIORITY REFERENCE TO RELATED APPLICATIONS

This application claims benefit of and hereby incorporates by reference provisional application Ser. No. 60/205,591, entitled "Computer Network Malicious Code Run-time Monitoring," filed on May 17, 2000 by inventors Nimrod Itzhak Vered, et al. This application is also a Continuation-In-Part of and hereby incorporates by reference patent application Ser. No. 09/539,667, now U.S. Pat. No. 6,804,780, entitled "System and Method for Protecting a Computer and a Network From Hostile Downloadables" filed on Mar. 30, 2000 by inventor Shlomo Touboul. This application is also a Continuation-In-Part of and hereby incorporates by reference patent application Ser. No. 09/551,302, now U.S. Pat. No. 6,480,962, entitled "System and Method for Protecting a Client During Runtime From Hostile Downloadables", filed on Apr. 18, 2000 by inventor Shlomo Touboul.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and methods for protecting network-connectable devices from undesirable downloadable operation.

2. Description of the Background Art

Advances in networking technology continue to impact an increasing number and diversity of users. The Internet, for example, already provides to expert, intermediate and even novice users the informational, product and service resources of over 100,000 interconnected networks owned by governments, universities, nonprofit groups, companies, etc. Unfortunately, particularly the Internet and other public networks have also become a major source of potentially system-fatal or otherwise damaging computer code commonly referred to as "viruses."

Efforts to forestall viruses from attacking networked computers have thus far met with only limited success at best. Typically, a virus protection program designed to identify and remove or protect against the initiating of known viruses is installed on a network firewall or individually networked computer. The program is then inevitably surmounted by some new virus that often causes damage to one or more computers. The damage is then assessed and, if isolated, the new virus is analyzed. A corresponding new virus protection program (or update thereof) is then developed and installed to combat the new virus, and the new program operates successfully until yet another new virus appears—and so on. Of course, damage has already typically been incurred.

To make matters worse, certain classes of viruses are not well recognized or understood, let alone protected against. It is observed by this inventor, for example, that Downloadable information comprising program code can include distributable components (e.g. Java™ applets and JavaScript scripts, ActiveX™ controls, Visual Basic, add-ins and/or others). It can also include, for example, application programs, Trojan horses, multiple compressed programs such as zip or meta files, among others. U.S. Pat. No. 5,983,348 to Shuang, however, teaches a protection system for protecting against only distributable components including "Java applets or ActiveX controls", and further does so using resource intensive and high bandwidth static Downloadable content and operational analysis, and modification of the Downloadable component; Shuang further fails to detect or protect against additional program code included within a tested Downloadable. U.S. Pat. No. 5,974,549 to Golan teaches a protection system that further focuses only on protecting against ActiveX controls and not other distributable components, let alone other Downloadable types. U.S. Pat. No. 6,167,520 to Touboul enables more accurate protection than Shuang or Golan, but lacks the greater flexibility and efficiency taught herein, as do Shuang and Golan.

Accordingly, there remains a need for efficient, accurate and flexible protection of computers and other network connectable devices from malicious Downloadables.

SUMMARY OF THE INVENTION

The present invention provides protection systems and methods capable of protecting a personal computer ("PC") or other persistently or even intermittently network accessible devices or processes from harmful, undesirable, suspicious or other "malicious" operations that might otherwise be effectuated by remotely operable code. While enabling the capabilities of prior systems, the present invention is not nearly so limited, resource intensive or inflexible, and yet enables more reliable protection. For example, remotely operable code that is protectable against can include downloadable application programs, Trojan horses and program code groupings, as well as software "components", such as Java™ applets, ActiveX™ controls, JavaScript™/Visual Basic scripts, add-ins, etc., among others. Protection can also be provided in a distributed interactively, automatically or mixed configurable manner using protected client, server or other parameters, redirection, local/remote logging, etc., and other server/client based protection measures can also be separately and/or interoperably utilized, among other examples.

In one aspect, embodiments of the invention provide for determining, within one or more network "servers" (e.g. fireballs, resources, gateways, email relays or other devices/processes that are capable of receiving-and-transferring a Downloadable) whether received information includes executable code (and is a "Downloadable"). Embodiments also provide for delivering static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables. Further client-based or remote protection code/policies can also be utilized in a distributed manner. Embodiments also provide for causing the mobile protection code to be executed within a Downloadable-destination in a manner that enables various Downloadable operations to be detected, intercepted or further responded to via protection operations. Additional server/information-destination device security or other protection is also enabled, among still further aspects.

A protection engine according to an embodiment of the invention is operable within one or more network servers, firewalls or other network connectable information re-communicating devices (as are referred to herein summarily one or more "servers" or "re-communicators"). The protection engine includes an information monitor for monitoring information received by the server, and a code detection engine for determining whether the received information includes executable code. The protection engine also includes a packaging engine for causing a sandboxed package, typically including mobile protection code and downloadable protection policies to be sent to a Downloadable-

destination in conjunction with the received information, if the received information is determined to be a Downloadable.

A sandboxed package according to an embodiment of the invention is receivable by and operable with a remote Downloadable-destination. The sandboxed package includes mobile protection code ("MPC") for causing one or more predetermined malicious operations or operation combinations of a Downloadable to be monitored or otherwise intercepted. The sandboxed package also includes protection policies (operable alone or in conjunction with further Downloadable-destination stored or received policies/MPCs) for causing one or more predetermined operations to be performed if one or more undesirable operations of the Downloadable is/are intercepted. The sandboxed package can also include a corresponding Downloadable and can provide for initiating the Downloadable in a protective "sandbox". The MPC/policies can further include a communicator for enabling further MPC/policy information or "modules" to be utilized and/or for event logging or other purposes.

A sandbox protection system according to an embodiment of the invention comprises an installer for enabling a received MPC to be executed within a Downloadable-destination (device/process) and further causing a Downloadable application program, distributable component or other received downloadable code to be received and installed within the Downloadable-destination. The protection system also includes a diverter for monitoring one or more operation attempts of the Downloadable, an operation analyzer for determining one or more responses to the attempts, and a security enforcer for effectuating responses to the monitored operations. The protection system can further include one or more security policies according to which one or more protection system elements are operable automatically (e.g. programmatically) or in conjunction with user intervention (e.g. as enabled by the security enforcer). The security policies can also be configurable/extensible in accordance with further downloadable and/or Downloadable-destination information.

A method according to an embodiment of the invention includes receiving downloadable information, determining whether the downloadable information includes executable code, and causing a mobile protection code and security policies to be communicated to a network client in conjunction with security policies and the downloadable information if the downloadable information is determined to include executable code. The determining can further provide multiple tests for detecting, alone or together, whether the downloadable information includes executable code.

A further method according to an embodiment of the invention includes forming a sandboxed package that includes mobile protection code ("MPC"), protection policies, and a received, detected-Downloadable, and causing the sandboxed package to be communicated to and installed by a receiving device or process ("user device") for responding to one or more malicious operation attempts by the detected-Downloadable from within the user device. The MPC/policies can further include a base "module" and a "communicator" for enabling further up/downloading of one or more further "modules" or other information (e.g. events, user/user device information, etc.).

Another method according to an embodiment of the invention includes installing, within a user device, received mobile protection code ("MPC") and protection policies in conjunction with the user device receiving a downloadable application program, component or other Downloadable(s). The method also includes determining, by the MPC, a resource access attempt by the Downloadable, and initiating, by the MPC, one or more predetermined operations corresponding to the attempt. (Predetermined operations can, for example, comprise initiating user, administrator, client, network or protection system determinable operations, including but not limited to modifying the Downloadable operation, extricating the Downloadable, notifying a user/another, maintaining a local/remote log, causing one or more MPCs/policies to be downloaded, etc.)

Advantageously, systems and methods according to embodiments of the invention enable potentially damaging, undesirable or otherwise malicious operations by even unknown mobile code to be detected, prevented, modified and/or otherwise protected against without modifying the mobile code. Such protection is further enabled in a manner that is capable of minimizing server and client resource requirements, does not require pre-installation of security code within a Downloadable-destination, and provides for client specific or generic and readily updateable security measures to be flexibly and efficiently implemented. Embodiments further provide for thwarting efforts to bypass security measures (e.g. by "hiding" undesirable operation causing information within apparently inert or otherwise "friendly" downloadable information) and/or dividing or combining security measures for even greater flexibility and/or efficiency.

Embodiments also provide for determining protection policies that can be downloaded and/or ascertained from other security information (e.g. browser settings, administrative policies, user input, uploaded information, etc.). Different actions in response to different Downloadable operations, clients, users and/or other criteria are also enabled, and embodiments provide for implementing other security measures, such as verifying a downloadable source, certification, authentication, etc. Appropriate action can also be accomplished automatically (e.g. programmatically) and/or in conjunction with alerting one or more users/administrators, utilizing user input, etc. Embodiments further enable desirable Downloadable operations to remain substantially unaffected, among other aspects.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1*a* is a block diagram illustrating a network system in accordance with an embodiment of the present invention;

FIG. 1*b* is a block diagram illustrating a network subsystem example in accordance with an embodiment of the invention;

FIG. 1*c* is a block diagram illustrating a further network subsystem example in accordance with an embodiment of the invention;

FIG. 2 is a block diagram illustrating a computer system in accordance with an embodiment of the invention;

FIG. 3 is a flow diagram broadly illustrating a protection system host according to an embodiment of the invention;

FIG. 4 is a block diagram illustrating a protection engine according to an embodiment of the invention;

FIG. 5 is a block diagram illustrating a content inspection engine according to an embodiment of the invention;

FIG. 6*a* is a block diagram illustrating protection engine parameters according to an embodiment of the invention;

FIG. 6*b* is a flow diagram illustrating a linking engine use in conjunction with ordinary, compressed and distributable sandbox package utilization, according to an embodiment of the invention;

FIG. **7***a* is a flow diagram illustrating a sandbox protection system operating within a destination system, according to an embodiment of the invention;

FIG. **7***b* is a block diagram illustrating memory allocation usable in conjunction with the protection system of FIG. **7***a*, according to an embodiment of the invention;

FIG. **8** is a block diagram illustrating a mobile protection code according to an embodiment of the invention;

FIG. **9** is a flowchart illustrating a server based protection method according to an embodiment of the invention;

FIG. **10***a* is a flowchart illustrating method for determining if a potential-Downloadable includes or is likely to include executable code, according to an embodiment of the invention;

FIG. **10***b* is a flowchart illustrating a method for forming a protection agent, according to an embodiment of the invention;

FIG. **11** is a flowchart illustrating a method for protecting a Downloadable destination according to an embodiment of the invention;

FIG. **12***a* is a flowchart illustrating a method for forming a Downloadable access interceptor according to an embodiment of the invention; and

FIG. **12***b* is a flowchart illustrating a method for implementing mobile protection policies according to an embodiment of the invention.

DETAILED DESCRIPTION

In providing malicious mobile code runtime monitoring systems and methods, embodiments of the invention enable actually or potentially undesirable operations of even unknown malicious code to be efficiently and flexibly avoided. Embodiments provide, within one or more "servers" (e.g. firewalls, resources, gateways, email relays or other information re-communicating devices), for receiving downloadable-information and detecting whether the downloadable-information includes one or more instances of executable code (e.g. as with a Trojan horse, zip/meta file etc.). Embodiments also provide for separately or interoperably conducting additional security measures within the server, within a Downloadable-destination of a detected-Downloadable, or both.

Embodiments further provide for causing mobile protection code ("MPC") and downloadable protection policies to be communicated to, installed and executed within one or more received information destinations in conjunction with a detected-Downloadable. Embodiments also provide, within an information-destination, for detecting malicious operations of the detected-Downloadable and causing responses thereto in accordance with the protection policies (which can correspond to one or more user, Downloadable, source, destination, or other parameters), or further downloaded or downloadable-destination based policies (which can also be configurable or extensible). (Note that the term "or", as used herein, is generally intended to mean "and/or" unless otherwise indicated.)

FIGS. **1***a* through **1***c* illustrate a computer network system **100** according to an embodiment of the invention. FIG. **1***a* broadly illustrates system **100**, while FIGS. **1***b* and **1***c* illustrate exemplary protectable subsystem implementations corresponding with system **104** or **106** of FIG. **1***a*.

Beginning with FIG. **1***a*, computer network system **100** includes an external computer network **101**, such as a Wide Area Network or "WAN" (e.g. the Internet), which is coupled to one or more network resource servers (summarily depicted as resource server-1 **102** and resource server-N **103**). Where external network **101** includes the Internet, resource servers 1-N (**102**, **103**) might provide one or more resources including web pages, streaming media, transaction-facilitating information, program updates or other downloadable information, summarily depicted as resources **121**, **131** and **132**. Such information can also include more traditionally viewed "Downloadables" or "mobile code" (i.e. distributable components), as well as downloadable application programs or other further Downloadables, such as those that are discussed herein. (It will be appreciated that interconnected networks can also provide various other resources as well.)

Also coupled via external network **101** are subsystems **104**–**106**. Subsystems **104**–**106** can, for example, include one or more servers, personal computers ("PCs"), smart appliances, personal information managers or other devices/processes that are at least temporarily or otherwise intermittently directly or indirectly connectable in a wired or wireless manner to external network **101** (e.g. using a dialup, DSL, cable modem, cellular connection, IR/RF, or various other suitable current or future connection alternatives). One or more of subsystems **104**–**106** might further operate as user devices that are connectable to external network **101** via an internet service provider ("ISP") or local area network ("LAN"), such as a corporate intranet, or home, portable device or smart appliance network, among other examples.

FIG. **1***a* also broadly illustrates how embodiments of the invention are capable of selectively, modifiably or extensibly providing protection to one or more determinable ones of networked subsystems **104**–**106** or elements thereof (not shown) against potentially harmful or other undesirable ("malicious") effects in conjunction with receiving downloadable information. "Protected" subsystem **104**, for example, utilizes a protection in accordance with the teachings herein, while "unprotected" subsystem-N **105** employs no protection, and protected subsystem-M **106** might employ one or more protections including those according to the teachings herein, other protection, or some combination.

System **100** implementations are also capable of providing protection to redundant elements **107** of one or more of subsystems **104**–**106** that might be utilized, such as backups, failsafe elements, redundant networks, etc. Where included, such redundant elements are also similarly protectable in a separate, combined or coordinated manner using embodiments of the present invention either alone or in conjunction with other protection mechanisms. In such cases, protection can be similarly provided singly, as a composite of component operations or in a backup fashion. Care should, however, be exercised to avoid potential repeated protection engine execution corresponding to a single Downloadable; such "chaining" can cause a Downloadable to operate incorrectly or not at all, unless a subsequent detection engine is configured to recognize a prior packaging of the Downloadable.

FIGS. **1***b* and **1***c* further illustrate, by way of example, how protection systems according to embodiments of the invention can be utilized in conjunction with a wide variety of different system implementations. In the illustrated examples, system elements are generally configurable in a manner commonly referred to as a "client-server" configuration, as is typically utilized for accessing Internet and many other network resources. For clarity sake, a simple client-server configuration will be presumed unless otherwise indicated. It will be appreciated, however, that other configurations of interconnected elements might also be utilized (e.g. peer-peer, routers, proxy servers, networks,

converters, gateways, services, network reconfiguring elements, etc.) in accordance with a particular application.

The FIG. **1***b* example shows how a suitable protected system **104***a* (which can correspond to subsystem-1 **104** or subsystem-M **106** of FIG. 1) can include a protection-initiating host "server" or "re-communicator" (e.g. ISP server **140***a*), one or more user devices or "Downloadable-destinations" **145**, and zero or more redundant elements (which elements are summarily depicted as redundant client device/process **145***a*). In this example, ISP server **140***a* includes one or more email, Internet or other servers **141***a*, or other devices or processes capable of transferring or otherwise "re-communicating" downloadable information to user devices **145**. Server **141***a* further includes protection engine or "PE" **142***a*, which is capable of supplying mobile protection code ("MPC") and protection policies for execution by client devices **145**. One or more of user devices **145** can further include a respective one or more clients **146** for utilizing information received via server **140***a*, in accordance with which MPC and protection policies are operable to protect user devices **145** from detrimental, undesirable or otherwise "malicious" operations of downloadable information also received by user device **145**.

The FIG. **1***c* example shows how a further suitable protected system **104***b* can include, in addition to a "re-communicator", such as server **142***b*, a firewall **143***c* (e.g. as is typically the case with a corporate intranet and many existing or proposed home/smart networks.) In such cases, a server **141***b* or firewall **143** can operate as a suitable protection engine host. A protection engine can also be implemented in a more distributed manner among two or more protection engine host systems or host system elements, such as both of server **141***b* and firewall **143**, or in a more integrated manner, for example, as a standalone device. Redundant system or system protection elements can also be similarly provided in a more distributed or integrated manner (see above).

System **104***b* also includes internal network **144** and user devices **145**. User devices **145** further include a respective one or more clients **146** for utilizing information received via server **140***a*, in accordance with which the MPCs or protection policies are operable. (As in the previous example, one or more of user devices **145** can also include or correspond with similarly protectable redundant system elements, which are not shown.)

It will be appreciated that the configurations of FIGS. **1***a*–**1***c* are merely exemplary. Alternative embodiments might, for example, utilize other suitable connections, devices or processes. One or more devices can also be configurable to operate as a network server, firewall, smart router, a resource server servicing deliverable third-party/manufacturer postings, a user device operating as a firewall/server, or other information-suppliers or intermediaries (i.e. as a "re-communicator" or "server") for servicing one or more further interconnected devices or processes or interconnected levels of devices or processes. Thus, for example, a suitable protection engine host can include one or more devices or processes capable of providing or supporting the providing of mobile protection code or other protection consistent with the teachings herein. A suitable information-destination or "user device" can further include one or more devices or processes (such as email, browser or other clients) that are capable of receiving and initiating or otherwise hosting a mobile code execution.

FIG. **2** illustrates an exemplary computing system **200**, that can comprise one or more of the elements of FIGS. **1***a* through **1***c*. While other application-specific alternatives might be utilized, it will be presumed for clarity sake that system **100** elements (FIGS. **1***a–c*) are implemented in hardware, software or some combination by one or more processing systems consistent therewith, unless otherwise indicated.

Computer system **200** comprises elements coupled via communication channels (e.g. bus **201**) including one or more general or special purpose processors **202**, such as a Pentium® or Power PC®, digital signal processor ("DSP"), etc. System **200** elements also include one or more input devices **203** (such as a mouse, keyboard, microphone, pen, etc.), and one or more output devices **204**, such as a suitable display, speakers, actuators, etc., in accordance with a particular application.

System **200** also includes a computer readable storage media reader **205** coupled to a computer readable storage medium **206**, such as a storage/memory device or hard or removable storage/memory media; such devices or media are further indicated separately as storage device **208** and memory **209**, which can include hard disk variants, floppy/compact disk variants, digital versatile disk ("DVD") variants, smart cards, read only memory, random access memory, cache memory, etc., in accordance with a particular application. One or more suitable communication devices **207** can also be included, such as a modem, DSL, infrared or other suitable transceiver, etc. for providing inter-device communication directly or via one or more suitable private or public networks that can include but are not limited to those already discussed.

Working memory further includes operating system ("OS") elements and other programs, such as application programs, mobile code, data, etc. for implementing system **100** elements that might be stored or loaded therein during use. The particular OS can vary in accordance with a particular device, features or other aspects in accordance with a particular application (e.g. Windows, Mac, Linux, Unix or Palm OS variants, a proprietary OS, etc.). Various programming languages or other tools can also be utilized, such as C++, Java, Visual Basic, etc. As will be discussed, embodiments can also include a network client such as a browser or email client, e.g. as produced by Netscape, Microsoft or others, a mobile code executor such as an OS task manager, Java Virtual Machine ("JVM"), etc., and an application program interface ("API"), such as a Microsoft Windows or other suitable element in accordance with the teachings herein. (It will also become apparent that embodiments might also be implemented in conjunction with a resident application or combination of mobile code and resident application components.)

One or more system **200** elements can also be implemented in hardware, software or a suitable combination. When implemented in software (e.g. as an application program, object, downloadable, servlet, etc. in whole or part), a system **200** element can be communicated transitionally or more persistently from local or remote storage to memory (or cache memory, etc.) for execution, or another suitable mechanism can be utilized, and elements can be implemented in compiled or interpretive form. Input, intermediate or resulting data or functional elements can further reside more transitionally or more persistently in a storage media, cache or more persistent volatile or non-volatile memory, (e.g. storage device **207** or memory **208**) in accordance with a particular application.

FIG. **3** illustrates an interconnected re-communicator **300** generally consistent with system **140***b* of FIG. **1**, according to an embodiment of the invention. As with system **140***b*, system **300** includes a server **301**, and can also include a

firewall **302**. In this implementation, however, either server **301** or firewall **302** (if a firewall is used) can further include a protection engine (**310** or **320** respectively). Thus, for example, an included firewall can process received information in a conventional manner, the results of which can be further processed by protection engine **310** of server **301**, or information processed by protection engine **320** of an included firewall **302** can be processed in a conventional manner by server **301**. (For clarity sake, a server including a singular protection engine will be presumed, with or without a firewall, for the remainder of the discussion unless otherwise indicated. Note, however, that other embodiments consistent with the teachings herein might also be utilized.)

FIG. **3** also shows how information received by server **301** (or firewall **302**) can include non-executable information, executable information or a combination of non-executable and one or more executable code portions (e.g. so-called Trojan horses that include a hostile Downloadable within a friendly one, combined, compressed or otherwise encoded files, etc.). Particularly such combinations will likely remain undetected by a firewall or other more conventional protection systems. Thus, for convenience, received information will also be referred to as a "potential-Downloadable", and received information found to include executable code will be referred to as a "Downloadable" or equivalently as a "detected-Downloadable" (regardless of whether the executable code includes one or more application programs, distributable "components" such as Java, ActiveX, add-in, etc.).

Protection engine **310** provides for detecting whether received potential-Downloadables include executable code, and upon such detection, for causing mobile protection code ("MPC") to be transferred to a device that is a destination of the potential-Downloadable (or "Downloadable-destination"). Protection engine **310** can also provide protection policies in conjunction with the MPC (or thereafter as well), which MPC/policies can be automatically (e.g. programmatically) or interactively configurable in accordance user, administrator, downloadable source, destination, operation, type or various other parameters alone or in combination (see below). Protection engine **310** can also provide or operate separately or interoperably in conjunction with one or more of certification, authentication, downloadable tagging, source checking, verification, logging, diverting or other protection services via the MPC, policies, other local/remote server or destination processing, etc. (e.g. which can also include protection mechanisms taught by the above-noted prior applications; see FIG. **4**).

Operationally, protection engine **310** of server **301** monitors information received by server **301** and determines whether the received information is deliverable to a protected destination, e.g. using a suitable monitor/data transfer mechanism and comparing a destination-address of the received information to a protected destination set, such as a protected destinations list, array, database, etc. (All deliverable information or one or more subsets thereof might also be monitored.) Protection engine **310** further analyzes the potential-Downloadable and determines whether the potential-Downloadable includes executable code. If not, protection engine **310** enables the not executable potential-Downloadable **331** to be delivered to its destination in an unaffected manner.

In conjunction with determining that the potential-Downloadable is a detected-Downloadable, protection engine **310** also causes mobile protection code or "MPC" **341** to be communicated to the Downloadable-destination of the Downloadable, more suitably in conjunction with the detected-Downloadable **343** (see below). Protection engine **310** further causes downloadable protection policies **342** to be delivered to the Downloadable-destination, again more suitably in conjunction with the detected-Downloadable. Protection policies **342** provide parameters (or can additionally or alternatively provide additional mobile code) according to which the MPC is capable of determining or providing applicable protection to a Downloadable-destination against malicious Downloadable operations.

(One or more "checked", tag, source, destination, type, detection or other security result indicators, which are not shown, can also be provided as corresponding to determined non-Downloadables or Downloadables, e.g. for testing, logging, further processing, further identification tagging or other purposes in accordance with a particular application.)

Further MPCs, protection policies or other information are also deliverable to a the same or another destination, for example, in accordance with communication by an MPC/protection policies already delivered to a downloadable-destination. Initial or subsequent MPCs/policies can further be selected or configured in accordance with a Downloadable-destination indicated by the detected-Downloadable, destination-user or administrative information, or other information providable to protection engine **310** by a user, administrator, user system, user system examination by a communicated MPC, etc. (Thus, for example, an initial MPC/policies can also be initially provided that are operable with or optimized for more efficient operation with different Downloadable-destinations or destination capabilities.)

While integrated protection constraints within the MPC might also be utilized, providing separate protection policies has been found to be more efficient, for example, by enabling more specific protection constraints to be more easily updated in conjunction with detected-Downloadable specifics, post-download improvements, testing, etc. Separate policies can further be more efficiently provided (e.g. selected, modified, instantiated, etc.) with or separately from an MPC, or in accordance with the requirements of a particular user, device, system, administration, later improvement, etc., as might also be provided to protection engine **310** (e.g. via user/MPC uploading, querying, parsing a Downloadable, or other suitable mechanism implemented by one or more servers or Downloadable-destinations).

(It will also become apparent that performing executable code detection and communicating to a downloadable-Destination an MPC and any applicable policies as separate from a detected-Downloadable is more accurate and far less resource intensive than, for example, performing content and operation scanning, modifying a Downloadable, or providing completely Downloadable-destination based security.)

System **300** enables a single or extensible base-MPC to be provided, in anticipation or upon receipt of a first Downloadable, that is utilized thereafter to provide protection of one or more Downloadable-destinations. It is found, however, that providing an MPC upon each detection of a Downloadable (which is also enabled) can provide a desirable combination of configurability of the MPC/policies and lessened need for management (e.g. given potentially changing user/destination needs, enabling testing, etc.).

Providing an MPC upon each detection of a Downloadable also facilitates a lessened demand on destination resources, e.g. since information-destination resources used in executing the MPC/policies can be re-allocated following such use. Such alternatives can also be selectively, modifiably or extensibly provided (or further in accordance with other application-specific factors that might also apply.)

Thus, for example, a base-MPC or base-policies might be provided to a user device that is/are extensible via additionally downloadable "modules" upon server **301** detection of a Downloadable deliverable to the same user device, among other alternatives.

In accordance with a further aspect of the invention, it is found that improved efficiency can also be achieved by causing the MPC to be executed within a Downloadable-destination in conjunction with, and further, prior to initiation of the detected Downloadable. One mechanism that provides for greater compatibility and efficiency in conjunction with conventional client-based Downloadable execution is for a protection engine to form a sandboxed package **340** including MPC **341**, the detected-Downloadable **343** and any policies **342**. For example, where the Downloadable is a binary executable to be executed by an operating system, protection engine **310** forms a protected package by concatenating, within sandboxed package **340**, MPC **341** for delivery to a Downloadable-destination first, followed by protection policies **342** and Downloadable **343**. (Concatenation or techniques consistent therewith can also be utilized for providing a protecting package corresponding to a Java applet for execution by a JVM of a Downloadable-destination, or with regard to ActiveX controls, add-ins or other distributable components, etc.)

The above concatenation or other suitable processing will result in the following. Upon receipt of sandboxed package **340** by a compatible browser, email or other destination-client and activating of the package by a user or the destination-client, the operating system (or a suitable responsively initiated distributed component host) will attempt to initiate sandboxed package **340** as a single Downloadable. Such processing will, however, result in initiating the MPC **341** and—in accordance with further aspects of the invention—the MPC will initiate the Downloadable in a protected manner, further in accordance with any applicable included or further downloaded protection policies **342**. (While system **300** is also capable of ascertaining protection policies stored at a Downloadable-destination, e.g. by poll, query, etc. of available destination information, including at least initial policies within a suitable protecting package is found to avoid associated security concerns or inefficiencies.)

Turning to FIG. **4**, a protection engine **400** generally consistent with protection engine **310** (or **320**) of FIG. **3** is illustrated in accordance with an embodiment of the invention. Protection engine **400** comprises information monitor **401**, detection engine **402**, and protected packaging engine **403**, which further includes agent generator **431**, storage **404**, linking engine **405**, and transfer engine **406**. Protection engine **400** can also include a buffer **407**, for temporarily storing a received potential-Downloadable, or one or more systems for conducting additional authentication, certification, verification or other security processing (e.g. summarily depicted as security system **408**) Protection engine **400** can further provide for selectively re-directing, further directing, logging, etc. of a potential/detected Downloadable or information corresponding thereto in conjunction with detection, other security, etc., in accordance with a particular application.

(Note that FIG. **4**, as with other figures included herein, also depicts exemplary signal flow arrows; such arrows are provided to facilitate discussion, and should not be construed as exclusive or otherwise limiting.)

Information monitor **401** monitors potential-Downloadables received by a host server and provides the information via buffer **407** to detection engine **402** or to other system **400** elements. Information monitor **401** can be configured to monitor host server download operations in conjunction with a user or a user-device that has logged-on to the server, or to receive information via a server operation hook, servlet, communication channel or other suitable mechanism.

Information monitor **401** can also provide for transferring, to storage **404** or other protection engine elements, configuration information including, for example, user, MPC, protection policy, interfacing or other configuration information (e.g. see FIG. **6**). Such configuration information monitoring can be conducted in accordance with a user/device logging onto or otherwise accessing a host server, via one or more of configuration operations, using an applet to acquire such information from or for a particular user, device or devices, via MPC/policy polling of a user device, or via other suitable mechanisms.

Detection engine **402** includes code detector **421**, which receives a potential-Downloadable and determines, more suitably in conjunction with inspection parameters **422**, whether the potential-Downloadable includes executable code and is thus a "detected-Downloadable". (Code detector **421** can also include detection processors for performing file decompression or other "decoding", or such detection-facilitating processing as decryption, utilization/support of security system **408**, etc. in accordance with a particular application.)

Detection engine **402** further transfers a detected-downloadable ("XEQ") to protected packaging engine **403** along with indicators of such detection, or a determined non-executable ("NXEQ") to transfer engine **406**. (Inspection parameters **422** enable analysis criteria to be readily updated or varied, for example, in accordance with particular source, destination or other potential Downloadable impacting parameters, and are discussed in greater detail with reference to FIG. **5**). Detection engine **402** can also provide indicators for delivery of initial and further MPCs/policies, for example, prior to or in conjunction with detecting a Downloadable and further upon receipt of an indicator from an already downloaded MPC/policy. A downloaded MPC/policy can further remain resident at a user device with further modules downloaded upon or even after delivery of a sandboxed package. Such distribution can also be provided in a configurable manner, such that delivery of a complete package or partial packages are automatically or interactively determinable in accordance with user/administrative preferences/policies, among other examples.

Packaging engine **403** provides for generating mobile protection code and protection policies, and for causing delivery thereof (typically with a detected-Downloadable) to a Downloadable-destination for protecting the Downloadable-destination against malicious operation attempts by the detected Downloadable. In this example, packaging engine **403** includes agent generator **431**, storage **404** and linking engine **405**.

Agent generator **431** includes an MPC generator **432** and a protection policy generator **433** for "generating" an MPC and a protection policy (or set of policies) respectively upon receiving one or more "generate MPC/policy" indicators from detection engine **402**, indicating that a potential-Downloadable is a detected-Downloadable. MPC generator **432** and protection policy generator **433** provide for generating MPCs and protection policies respectively in accordance with parameters retrieved from storage **404**. Agent generator **431** is further capable of providing multiple MPCs/policies, for example, the same or different MPCs/policies in accordance with protecting ones of multiple executables within a

zip file, or for providing initial MPCs/policies and then further MPCs/policies or MPC/policy "modules" as initiated by further indicators such as given above, via an indicator of an already downloaded MPC/policy or via other suitable mechanisms. (It will be appreciated that pre-constructed MPCs/policies or other processing can also be utilized, e.g. via retrieval from storage **404**, but with a potential decrease in flexibility.)

MPC generator **432** and protection policy generator **433** are further configurable. Thus, for example, more generic MPCs/policies can be provided to all or a grouping of serviced destination-devices (e.g. in accordance with a similarly configured/administered intranet), or different MPCs/policies that can be configured in accordance with one or more of user, network administration, Downloadable-destination or other parameters (e.g. see FIG. **6**). As will become apparent, a resulting MPC provides an operational interface to a destination device/process. Thus, a high degree of flexibility and efficiency is enabled in providing such an operational interface within different or differently configurable user devices/processes or other constraints.

Such configurability further enables particular policies to be utilized in accordance with a particular application (e.g. particular system uses, access limitations, user interaction, treating application programs or Java components from a particular known source one way and unknown source ActiveX components, or other considerations). Agent generator **431** further transfers a resulting MPC and protection policy pair to linking engine **405**.

Linking engine **405** provides for forming from received component elements (see above) a sandboxed package that can include one or more initial or complete MPCs and applicable protection policies, and a Downloadable, such that the sandboxed package will protect a receiving Downloadable-destination from malicious operation by the Downloadable. Linking engine **405** is implementable in a static or configurable manner in accordance, for example, with characteristics of a particular user device/process stored intermittently or more persistently in storage **404**. Linking engine **405** can also provide for restoring a Downloadable, such as a compressed, encrypted or otherwise encoded file that has been decompressed, decrypted or otherwise decoded via detection processing (e.g. see FIG. **6***b*).

It is discovered, for example, that the manner in which the Windows OS initiates a binary executable or an ActiveX control can be utilized to enable protected initiation of a detected-Downloadable. Linking engine **405** is, for example, configurable to form, for an ordinary single-executable Downloadable (e.g. an application program, applet, etc.) a sandboxed package **340** as a concatenation of ordered elements including an MPC **341**, applicable policies **342** and the Downloadable or "XEQ" **343** (e.g. see FIG. **4**).

Linking engine **405** is also configurable to form, for a Downloadable received by a server as a compressed single or multiple-executable Downloadable such as a zipped or meta file, a protecting package **340** including one or more MPCs, applicable policies and the one or more included executables of the Downloadable. For example, a sandboxed package can be formed in which a single MPC and policies precede and thus will affect all such executables as a result of inflating and installation. An MPC and applicable policies can also, for example, precede each executable, such that each executable will be separately sandboxed in the same or a different manner according to MPC/policy configuration (see above) upon inflation and installation. (See also FIGS. **5** and **6**)

Linking engine is also configurable to form an initial MPC, MPC-policy or sandboxed package (e.g. prior to upon receipt of a downloadable) or an additional MPC, MPC-policy or sandboxed package (e.g. upon or following receipt of a downloadable), such that suitable MPCs/policies can be provided to a Downloadable-destination or other destination in a more distributed manner. In this way, requisite bandwidth or destination resources can be minimized (via two or more smaller packages) in compromise with latency or other considerations raised by the additional required communication.

A configurable linking engine can also be utilized in accordance with other requirements of particular devices/processes, further or different elements or other permutations in accordance with the teachings herein. (It might, for example be desirable to modify the ordering of elements, to provide one or more elements separately, to provide additional information, such as a header, etc., or perform other processing in accordance with a particular device, protocol or other application considerations.)

Policy/authentication reader-analyzer **481** summarily depicts other protection mechanisms that might be utilized in conjunction with Downloadable detection, such as already discussed, and that can further be configurable to operate in accordance with policies or parameters (summarily depicted by security/authentication policies **482**). Integration of such further protection in the depicted configuration, for example, enables a potential-Downloadable from a known unfriendly source, a source failing authentication or a provided-source that is confirmed to be fictitious to be summarily discarded, otherwise blocked, flagged, etc. (with or without further processing). Conversely, a potential-Downloadable from a known friendly source (or one confirmed as such) can be transferred with or without further processing in accordance with particular application considerations. (Other configurations including pre or post Downloadable detection mechanisms might also be utilized.)

Finally, transfer engine **406** provides for receiving and causing linking engine **405** (or other protection) results to be transferred to a destination user device/process. As depicted, transfer engine **406** is configured to receive and transfer a Downloadable, a determined non-executable or a sandboxed package. However, transfer engine **406** can also be provided in a more configurable manner, such as was already discussed for other system **400** elements. (Any one or more of system **400** elements might be configurably implemented in accordance with a particular application.) Transfer engine **406** can perform such transfer, for example, by adding the information to a server transfer queue (not shown) or utilizing another suitable method.

Turning to FIG. **5** with reference to FIG. **4**, a code detector **421** example is illustrated in accordance with an embodiment of the invention. As shown, code detector **421** includes data fetcher **501**, parser **502**, file-type detector **503**, inflator **504** and control **506**; other depicted elements. While implementable and potentially useful in certain instances, are found to require substantial overhead, to be less accurate in certain instances (see above) and are not utilized in a present implementation; these will be discussed separately below. Code detector elements are further configurable in accordance with stored parameters retrievable by data fetcher **501**. (A coupling between data fetcher **501** and control **506** has been removed for clarity sake.)

Data fetcher **501** provides for retrieving a potential-Downloadable or portions thereof stored in buffer **407** or parameters from storage **404**, and communicates such information or parameters to parser **502**. Parser **502** receives a

potential-Downloadable or portions thereof from data fetcher **501** and isolates potential-Downloadable elements, such as file headers, source, destination, certificates, etc. for use by further processing elements.

File type detector **502** receives and determines whether the potential-Downloadable (likely) is or includes an executable file type. File-reader **502** can, for example, be configured to analyze a received potential-Downloadable for a file header, which is typically included in accordance with conventional data transfer protocols, such as a portable executable or standard ".exe" file format for Windows OS application programs, a Java class header for Java applets, and so on for other applications, distributed components, etc. "Zipped", meta or other compressed files, which might include one or more executables, also typically provide standard single or multi-level headers that can be read and used to identify included executable code (or other included information types). File type detector **502** is also configurable for analyzing potential-Downloadables for all potential file type delimiters or a more limited subset of potential file type delimiters (e.g. ".exe" or ".com" in conjunction with a DOS or Microsoft Windows OS Downloadable-destination).

Known file type delimiters can, for example, be stored in a more temporary or more persistent storage (e.g. storage **404** of FIG. **4**) which file type detector **502** can compare to a received potential-Downloadable. (Such delimiters can thus also be updated in storage **404** as a new file type delimiter is provided, or a more limited subset of delimiters can also be utilized in accordance with a particular Downloadable-destination or other considerations of a particular application.) File type detector **502** further transfers to controller **506** a detected file type indicator indicating that the potential-Downloadable includes or does not include (i.e. or likely include) an executable file type.

In this example, the aforementioned detection processor is also included as predetection processor or, more particularly, a configurable file inflator **504**. File inflator **504** provides for opening or "inflating" compressed files in accordance with a compressed file type received from file type detector **503** and corresponding file opening parameters received from data fetcher **501**. Where a compressed file (e.g. a meta file) includes nested file type information not otherwise reliably provided in an overall file header or other information, inflator **504** returns such information to parser **502**. File inflator **504** also provides any now-accessible included executables to control **506** where one or more included files are to be separately packaged with an MPC or policies.

Control **506**, in this example, operates in accordance with stored parameters and provides for routing detected non-Downloadables or Downloadables and control information, and for conducting the aforementioned distributed downloading of packages to Downloadable-destinations. In the case of a non-Downloadable, for example, control **506** sends the non-Downloadable to transfer engine **406** (FIG. **4**) along with any indicators that might apply. For an ordinary single-executable Downloadable, control **506** sends control information to agent generator **431** and the Downloadable to linking engine **405** along with any other applicable indicators (see **641** of FIG. **6***b*). Control **506** similarly handles a compressed single-executable Downloadable or a multiple downloadable to be protected using a single sandboxed package. For a multiple-executable Downloadable, control **506** sends control information for each corresponding executable to agent generator agent generator **431**, and sends the executable to linking engine **405** along with controls and any applicable indicators, as in **643***b* of FIG. **6***b*. (The above assumes, however, that distributed downloading is not utilized; when used—according to applicable parameters—control **506** also operates in accordance with the following.)

Control **506** conducts distributed protection (e.g. distributed packaging) by providing control signals to agent generator **431**, linking engine **405** and transfer engine **406**. In the present example, control **506** initially sends controls to agent generator **431** and linking engine **405** (FIG. **4**) causing agent generator to generate an initial MPC and initial policies, and sends control and a detected-Downloadable to linking engine **405**. Linking engine **405** forms an initial sandboxed package, which transfer engine causes (in conjunction with further controls) to be downloaded to the Downloadable destination (**643***a* of FIG. **6***b*). An initial MPC within the sandboxed package includes an installer and a communicator and performs installation as indicated below. The initial MPC also communicates via the communicator controls to control **506** (FIG. **5**) in response to which control **506** similarly causes generation of MPC-M and policy-M modules **643***c*, which linking engine **405** links and transfer engine **406** causes to be sent to the Downloadable destination, and so on for any further such modules.

(It will be appreciated, however, that an initial package might be otherwise configured or sent prior to receipt of a Downloadable in accordance with configuration parameters or user interaction. Information can also be sent to other user devices, such as that of an administrator. Further MPCs/policies might also be coordinated by control **506** or other elements, or other suitable mechanisms might be utilized in accordance with the teachings herein.)

Regarding the remaining detection engine elements illustrated in FIG. **5**, where content analysis is utilized, parser **502** can also provide a Downloadable or portions thereof to content detector **505**. Content detector **505** can then provide one or more content analyses. Binary detector **551**, for example, performs detection of binary information; pattern detector **552** further analyzes the Downloadable for patterns indicating executable code, or other detectors can also be utilized. Analysis results therefrom can be used in an absolute manner, where a first testing result indicating executable code confirms Downloadable detection, which result is then sent to control **506**. Alternatively, however, composite results from such analyses can also be sent to control **506** for evaluation. Control **506** can further conduct such evaluation in a summary manner (determining whether a Downloadable is detected according to a majority or minimum number of indicators), or based on a weighting of different analysis results. Operation then continues as indicated above. (Such analysis can also be conducted in accordance with aspects of a destination user device or other parameters.)

FIG. **6***a* illustrates more specific examples of indicators/parameters and known (or "knowledge base") elements that can be utilized to facilitate the above-discussed system **400** configurability and detection. For clarity sake, indicators, parameters and knowledge base elements are combined as indicated "parameters." It will be appreciated, however, that the particular parameters utilized can differ in accordance with a particular application, and indicators, parameters or known elements, where utilized, can vary and need not correspond exactly with one another. Any suitable explicit or referencing list, database or other storage structure(s) or storage structure configuration(s) can also be utilized to implement a suitable user/device based protection scheme, such as in the above examples, or other desired protection schema.

Executable parameters **601** comprise, in accordance with the above examples, executable file type parameters **611**,

executable code parameters **612** and code pattern parameters **613** (including known executable file type indicators, header/code indicators and patterns respectively, where code patterns are utilized). Use parameters **602** further comprise user parameters **621**, system parameters **622** and general parameters **623** corresponding to one or more users, user classifications, user-system correspondences or destination system, device or processes, etc. (e.g. for generating corresponding MPCs/policies, providing other protection, etc.). The remaining parameters include interface parameters **631** for providing MPC/policy (or further) configurability in accordance with a particular device or for enabling communication with a device user (see below), and other parameters **632**.

FIG. **6***b* illustrates a linking engine **405** according to an embodiment of the invention. As already discussed, linking engine **405** includes a linker for combining MPCs, policies or agents via concatination or other suitable processing in accordance with an OS, JVM or other host executor or other applicable factors that might apply. Linking engine **405** also includes the aforementioned post-detection processor which, in this example, comprises a compressor **508**. As noted, compressor **508** receives linked elements from linker **507** and, where a potential-Downloadable corresponds to a compressed file that was inflated during detection, re-forms the compressed file. (Known file information can be provided via configuration parameters, substantially reversal of inflating or another suitable method.) Encryption or other post-detection processing can also be conducted by linking engine **508**.

FIGS. **7***a*, **7***b* and **8** illustrate a "sandbox protection" system, as operable within a receiving destination-device, according to an embodiment of the invention.

Beginning with FIG. **7***a*, a client **146** receiving sandbox package **340** will "recognize" sandbox package **340** as a (mobile) executable and cause a mobile code installer **711** (e.g. an OS loader, JVM, etc.) to be initiated. Mobile code installer **711** will also recognize sandbox package **340** as an executable and will attempt to initiate sandbox package **340** at its "beginning." Protection engine **400** processing corresponding to destination **700** use of a such a loader, however, will have resulted in the "beginning" of sandbox package **340** as corresponding to the beginning of MPC **341**, as noted with regard to the above FIG. **4** example.

Such protection engine processing will therefore cause a mobile code installer (e.g. OS loader **711**, for clarity sake) to initiate MPC **341**. In other cases, other processing might also be utilized for causing such initiation or further protection system operation. Protection engine processing also enables MPC **341** to effectively form a protection "sandbox" around Downloadable (e.g. detected-Downloadable or "XEQ") **343**, to monitor Downloadable **343**, intercept determinable Downloadable **343** operation (such as attempted accesses of Downloadable **343** to destination resources) and, if "malicious", to cause one or more other operations to occur (e.g. providing an alert, offloading the Downloadable, offloading the MPC, providing only limited resource access, possibly in a particular address space or with regard to a particularly "safe" resource or resource operation, etc.).

MPC **341**, in the present OS example, executes MPC element installation and installs any policies, causing MPC **341** and protection policies **342** to be loaded into a first memory space, P1. MPC **341** then initiates loading of Downloadable **343**. Such Downloadable initiation causes OS loader **711** to load Downloadable **343** into a further working memory space-P2 **703** along with an API import table ("IAT") **731** for providing Downloadable **631** with destination resource access capabilities. It is discovered, however that the IAT can be modified so that any call to an API can be redirected to a function within the MPC. The technique for modifying the IAT is documented within the MSDN (Microsoft Developers Network) Library CD in several articles. The technique is also different for each operating system (e.g. between Windows 9× and Windows NT), which can be accommodated by agent generator configurability, such as that given above. MPC **341** therefore has at least initial access to API IAT **731** of Downloadable **632**, and provides for diverting, evaluating and responding to attempts by Downloadable **632** to utilize system APIs **731**, or further in accordance with protection policies **342**. In addition to API diverting, MPC **341** can also install filter drivers, which can be used for controlling access to resources such as a Downloadable-destination file system or registry. Filter driver installation can be conducted as documented in the MSDN or using other suitable methods.

Turning to FIG. **8** with reference to FIG. **7***b*, an MPC **341** according to an embodiment of the invention includes a package extractor **801**, executable installer **802**, sandbox engine installer **803**, resource access diverter **804**, resource access (attempt) analyzer **805**, policy enforcer **806** and MPC de-installer **807**. Package extractor **801** is initiated upon initiation of MPC **341**, and extracts MPC **341** elements and protection policies **342**. Executable installer **802** further initiates installation of a Downloadable by extracting the downloadable from the protected package, and loading the process into memory in suspended mode (so it only loads into memory, but does not start to run). Such installation further causes the operating system to initialize the Downloadable's IAT **731** in the memory space of the downloadable process, P2, as already noted.

Sandbox engine installer **803** (running in process space P1) then installs the sandbox engine (**803**-**805**) and policies **342** into the downloadable process space P2. This is done in different way in each operating system (e.g. see above). Resource access diverter **804** further modifies those Downloadable-API IAT entries that correspond with protection policies **342**, thereby causing corresponding Downloadable accesses via Downloadable-API IAT **731** to be diverted resource access analyzer **805**.

During Downloadable operation, resource access analyzer or "RAA" **805** receives and determines a response to diverted Downloadable (i.e. "malicious") operations in accordance with corresponding protection policies of policies **342**. (RAA **805** or further elements, which are not shown, can further similarly provide for other security mechanisms that might also be implemented.) Malicious operations can for example include, in a Windows environment: file operations (e.g. reading, writing, deleting or renaming a file), network operations (e.g. listen on or connect to a socket, send/receive data or view intranet), OS registry or similar operations (read/write a registry item), OS operations (exit OS/client, kill or change the priority of a process/thread, dynamically load a class library), resource usage thresholds (e.g. memory, CPU, graphics), etc.

Policy enforcer **806** receives RAA **805** results and causes a corresponding response to be implemented, again according to the corresponding policies. Policy enforcer **806** can, for example, interact with a user (e.g. provide an alert, receive instructions, etc.), create a log file, respond, cause a response to be transferred to the Downloadable using "dummy" or limited data, communicate with a server or other networked device (e.g. corresponding to a local or remote administrator), respond more specifically with a better known Downloadable, verify accessibility or user/

system information (e.g. via local or remote information), even enable the attempted Downloadable access, among a wide variety of responses that will become apparent in view of the teachings herein.

The FIG. **9** flowchart illustrates a protection method according to an embodiment of the invention. In step **901**, a protection engine monitors the receipt, by a server or other re-communicator of information, and receives such information intended for a protected information-destination (i.e. a potential-Downloadable) in step **903**. Steps **905–911** depict an adjunct trustworthiness protection that can also be provided, wherein the protection engine determines whether the source of the received information is known to be "unfriendly" and, if so, prevents current (at least unaltered) delivery of the potential-Downloadable and provides any suitable alerts. (The protection engine might also continue to perform Downloadable detection and nevertheless enable delivery or protected delivery of a non-Downloadable, or avoid detection if the source is found to be "trusted", among other alternatives enabled by the teachings herein.)

If, in step **913**, the potential-Downloadable source is found to be of an unknown or otherwise suitably authenticated/certified source, then the protection engine determines whether the potential-Downloadable includes executable code in step **915**. If the potential-Downloadable does not include executable code, then the protection engine causes the potential-Downloadable to be delivered to the information-destination in its original form in step **917**, and the method ends. If instead the potential-Downloadable is found to include executable code in step **915** (and is thus a "detected-Downloadable"), then the protection engine forms a sandboxed package in step **919** and causes the protection agent to be delivered to the information-Destination in step **921**, and the method ends. As was discussed earlier, a suitable protection agent can include mobile protection code, policies and the detected-Downloadable (or information corresponding thereto).

The FIG. **10***a* flowchart illustrates a method for analyzing a potential-Downloadable, according to an embodiment of the invention. As shown, one or more aspects can provide useful indicators of the inclusion of executable code within the potential-Downloadable. In step **1001**, the protection engine determines whether the potential-Downloadable indicates an executable file type, for example, by comparing one or more included file headers for file type indicators (e.g. extensions or other descriptors). The indicators can be compared against all known file types executable by all protected Downloadable destinations, a subset, in accordance with file types executable or desirably executable by the Downloadable-destination, in conjunction with a particular user, in conjunction with available information or operability at the destination, various combinations, etc.

Where content analysis is conducted, in step **1003** of FIG. **10***a*, the protection engine analyzes the potential-Downloadable and determines in accordance therewith whether the potential-Downloadable does or is likely to include binary information, which typically indicates executable code. The protection engine further analyzes the potential-Downloadable for patterns indicative of included executable code in step **1003**. Finally, in step **1005**, the protection engine determines whether the results of steps **1001** and **1003** indicate that the potential-Downloadable more likely includes executable code (e.g. via weighted comparison of the results with a suitable level indicating the inclusion or exclusion of executable code). The protection engine, given a suitably high confidence indicator of the inclusion of executable code, treats the potential-Downloadable as a detected-Downloadable.

The FIG. **10***b* flowchart illustrates a method for forming a sandboxed package according to an embodiment of the invention. As shown, in step **1011**, a protection engine retrieves protection parameters and forms mobile protection code according to the parameters. The protection engine further, in step **1013**, retrieves protection parameters and forms protection policies according to the parameters. Finally, in step **1015**, the protection engine couples the mobile protection code, protection policies and received-information to form a sandboxed package. For example, where a Downloadable-destination utilizes a standard windows executable, coupling can further be accomplished via concatenating the MPC for delivery of MPC first, policies second, and received information third. (The protection parameters can, for example, include parameters relating to one or more of the Downloadable destination device/process, user, supervisory constraints or other parameters.)

The FIG. **11** flowchart illustrates how a protection method performed by mobile protection code ("MPC") according to an embodiment of the invention includes the MPC installing MPC elements and policies within a destination device in step **1101**. In step **1102**, the MPC loads the Downloadable without actually initiating it (i.e. for executables, it will start a process in suspended mode). The MPC further forms an access monitor or "interceptor" for monitoring or "intercepting" downloadable destination device access attempts within the destination device (according to the protection policies in step **1103**, and initiates a corresponding Downloadable within the destination device in step **1105**.

If, in step **1107**, the MPC determines, from monitored/intercepted information, that the Downloadable is attempting or has attempted a destination device access considered undesirable or otherwise malicious, then the MPC performs steps **1109** and **1111**; otherwise the MPC returns to step **1107**. In step **1109**, the MPC determines protection policies in accordance with the access attempt by the Downloadable, and in step **1111**, the MPC executes the protection policies. (Protection policies can, for example, be retrieved from a temporary, e.g. memory/cache, or more persistent storage.)

As shown in the FIG. **12***a* example, the MPC can provide for intercepting Downloadable access attempts by a Downloadable by installing the Downloadable (but not executing it) in step **1201**. Such installation will cause a Downloadable executor, such as a the Windows operating system, to provide all required interfaces and parameters (such as the IAT, process ID, etc.) for use by the Downloadable to access device resources of the host device. The MPC can thus cause Downloadable access attempts to be diverted to the MPC by modifying the Downloadable IAT, replacing device resource location indicators with those of the MPC (step **1203**).

The FIG. **12***b* example further illustrates an example of how the MPC can apply suitable policies in accordance with an access attempt by a Downloadable. As shown, the MPC receives the Downloadable access request via the modified IAT in step **1211**. The MPC further queries stored policies to determine a policy corresponding to the Downloadable access request in step **1213**.

The foregoing description of preferred embodiments of the invention is provided by way of example to enable a person skilled in the art to make and use the invention, and in the context of particular applications and requirements thereof. Various modifications to the embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodi-

ments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

What is claimed is:

1. A processor-based method, comprising:

receiving downloadable-information;

determining whether the downloadable-information includes executable code; and

causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code,

wherein the determining comprises performing one or more analyses of the downloadable-information, the analyses producing detection-indicators indicating whether a correspondence is detected between a downloadable-information characteristic and at least one respective executable code characteristic, and evaluating the detection-indicators to determine whether the downloadable-information includes executable code.

2. The method of claim 1, wherein at least one of the detection-indicators indicates a level of downloadable-information characteristic and executable code characteristic correspondence.

3. The method of claim 1, wherein the evaluating includes assigning a weighted level of importance to at least one of the indicators.

4. A processor-based method, comprising:

receiving downloadable-information;

determining whether the downloadable-information includes executable code; and

causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code,

wherein the causing mobile protection code to be communicated comprises forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be communicated to the at least one information-destination.

5. The method of claim 4, wherein the sandboxed package is formed such that the mobile protection code will be executed by the information-destination before the downloadable-information.

6. The method of claim 5, wherein the sandboxed package further includes protection policies according to which the mobile protection code is operable.

7. The method of claim 6, wherein the sandboxed package is formed for receipt by the information-destination such that the mobile protection code is received before the downloadable-information, and the downloadable information before the protection policies.

8. The method of claim 6, wherein the protection policies correspond with at least one of the information-destination and a user of the information destination.

9. A processor-based system, comprising:

an information monitor for receiving downloadable-information;

a content inspection engine communicatively coupled to the information monitor for determining whether the downloadable-information includes executable code; and

a packaging engine communicatively coupled to the content inspection engine for causing mobile protection code ("MPC") to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code,

wherein the content inspection engine comprises one or more downloadable-information analyzers for analyzing the downloadable-information, each analyzer producing therefrom a detection indicator indicating whether a downloadable-information characteristic corresponds with an executable code characteristic, and an inspection controller communicatively coupled to the analyzers for determining whether the indicators indicate that the downloadable-information includes executable code.

10. The system of claim 9, wherein at least one of the detection-indicators indicates a level of downloadable-information characteristic and executable code characteristic correspondence.

11. The system of claim 9, wherein the evaluating includes assigning a weighted level of importance to at least one of the detection-indicators.

12. A processor-based system, comprising:

an information monitor for receiving downloadable-information;

a content inspection engine communicatively coupled to the information monitor for determining whether the downloadable-information includes executable code; and

a packaging engine communicatively coupled to the content inspection engine for causing mobile protection code ("MPC") to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code,

wherein the packaging engine comprises an MPC generator for providing the MPC, a linking engine coupled to the MPC generator for forming a sandbox package including the MPC and the downloadable-information, and a transfer engine for causing the sandbox package to be communicated to the at least one information-destination.

13. The system of claim 12, wherein the packaging engine further comprises a policy generator communicatively coupled to the linking engine for providing protection policies according to which the MPC is operable.

14. The system of claim 13, wherein the sandboxed package is formed for receipt by the information-destination such that the mobile protection code is executed before the downloadable-information.

15. The system of claim 14, wherein the protection policies correspond with policies of at least one of the information-destination and a user of the information destination.

16. A processor-based method, comprising:

receiving, at an information re-communicator, downloadable-information, including executable code; and

causing mobile protection code to be executed by a mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code,

wherein the causing is accomplished by forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be delivered to the downloadable-information destination.

17. The method of claim **16**, wherein the sandboxed package further includes protection policies according to which the processing by the mobile protection code is conducted.

18. A sandboxed package formed according to the method of claim **17**.

19. The method of claim **17**, wherein the forming comprises generating the mobile protection code, generating the sandboxed package, and linking the mobile protection code, protection policies and downloadable-information.

20. The method of claim **19**, wherein the generating of at least one of the mobile protection code and the protection policies is conducted in accordance with one or more destination-characteristics of the destination.

21. The method of claim **20**, wherein the destination-characteristics include characteristics corresponding to at least one of a destination user, a destination device and a destination process.

22. A sandboxed package formed according to the method of claim **16**.

23. The method of claim **16**, wherein the causing the sandboxed package to be executed includes communicating the sandboxed package to a communication buffer of the information re-communicator.

24. The method of claim **16**, wherein the re-communicator is at least one of a firewall and a network server.

25. The method of claim **16**, wherein the sandboxed package has a same file type as the downloadable-information, thereby causing the mobile code executor to be unaware that the protected package is not a normal downloadable.

26. The method of claim **25**, wherein the sandboxed package is formed using concatenation of a mobile protection code, a policy, and a downloadable.

27. The method of claim **16**, wherein executing the mobile protection code at the destination causes downloadable interfaces to resources at the destination to be modified such that at least one attempted operation of the executable code is diverted to the mobile protection code.

28. A processor-based system, comprising:

receiving means for receiving, at an information re-communicator, downloadable-information, including executable code; and

mobile code means communicatively coupled to the receiving means for causing mobile protection code to be executed by a mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code,

wherein the causing is accomplished by forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be delivered to the downloadable-information destination.

29. The system of claim **28**, wherein the sandboxed package further includes protection policies according to which the processing by the mobile protection code is conducted.

30. The system of claim **29**, wherein the forming comprises generating the mobile protection code, generating the protection policies, and linking the mobile protection code, protection policies and downloadable-information.

31. The system of claim **30**, wherein the generating of at least one of the mobile protection code and the protection policies is conducted in accordance with one or more destination-characteristics of the destination.

32. The system of claim **31**, wherein the destination-characteristics include characteristics corresponding to at least one of a destination user, a destination device and a destination process.

33. The system of claim **28**, wherein the causing the sandboxed package to be executed includes communicating the sandboxed package to a communication buffer of the information re-communicator.

34. The system of claim **33**, wherein the re-communicator is at least one of a firewall and a network server.

35. The system of claim **34**, wherein executing the mobile protection code at the destination causes downloadable interfaces a resource at the destination to be modified such that at least one attempted operation of the executable code is diverted to the mobile protection code.

* * * * *

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation,	)	
Plaintiff,	)	
v.	)	C.A. No. 06-369-GMS
SECURE COMPUTING CORPORATION, a Delaware corporation; CYBERGUARD CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100,	)	DEMAND FOR JURY TRIAL
Defendants.	)	

ANSWER AND COUNTERCLAIMS OF DEFENDANTS SECURE COMPUTING CORPORATION, CYBERGUARD CORPORATION, AND WEBWASHER AG TO PLAINTIFF'S AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG (collectively referred to as "Secure Computing") for their Answer to Plaintiff's Amended Complaint For Patent Infringement ("Amended Complaint"), state as follows:

GENERAL DENIAL

Secure Computing denies each and every allegation, matter or thing contained in the Amended Complaint which is not expressly admitted, qualified or answered herein.

THE PARTIES

1. Secure Computing lacks sufficient knowledge to form a belief as to the truth or falsity of the allegations contained in paragraph 1 of the Amended Complaint and therefore denies the same.

2. Secure Computing admits the allegations of paragraph 2 of the Amended Complaint.

3. Secure Computing denies the allegations of paragraph 3 of the Amended Complaint.

4. Secure Computing denies the allegations of paragraph 4 of the Amended Complaint.

JURISDICTION AND VENUE

5. The allegations in paragraph 5 are legal conclusions and do not require a responsive pleading. To the extent a response is required, Secure Computing does not dispute that jurisdiction is proper under 28 U.S.C. §§ 1331 and 1338.

6. The allegations in paragraph 6 are legal conclusions and do not require a responsive pleading. To the extent a response is required, Secure Computing does not dispute that venue is proper under 28 U.S.C. §§ 1391(b) and (c) and/or under 28 U.S.C. § 1400(b) and that personal jurisdiction is proper over Defendants. Secure Computing denies that Defendants CyberGuard Corp. and Webwasher AG are Delaware corporations. Secure Computing denies that any of the Defendants have and continue to infringe, contributorily infringe and/or induce infringement of U.S. Patent No. 6,092,194, U.S. Patent No. 6,804,780, and U.S. Patent No. 7,058,822.

PLAINTIFF'S PATENT

7. Secure Computing admits that Exhibit A to the Amended Complaint is a copy of the '194 patent. Secure Computing denies any and all other allegations of paragraph 7 of the Amended Complaint.

8. Secure Computing admits that Exhibit B to the Amended Complaint is a copy of the '780 patent. Secure Computing denies any and all other allegations of paragraph 8 of the Amended Complaint.

9. Secure Computing admits that Exhibit C to the Amended Complaint is a copy of the '822 patent. Secure Computing denies any and all other allegations of paragraph 9 of the Amended Complaint.

10. Secure Computing denies the allegations of paragraph 10 of the Amended Complaint.

PATENT INFRINGEMENT

11. Secure Computing Corporation admits that it is in the business of developing and distributing network and systems security solutions to organizations. Secure Computing denies any and all other allegations of paragraph 11 of the Amended Complaint.

12. Secure Computing admits that Defendant CyberGuard was in the business of developing and distributing information security solutions, but denies that CyberGuard is currently engaging in business. Secure Computing denies any and all other allegations of paragraph 12 of the Amended Complaint.

13. Secure Computing admits that Defendant Webwasher AG was in the business of developing and distributing Internet and email content security and filtering solutions, but denies that Webwasher AG is currently engaging in business. Secure Computing denies any and all other allegations of paragraph 13 of the Amended Complaint.

FIRST CAUSE OF ACTION

(Infringement of the '194 Patent)

14. Secure Computing admits that in paragraph 14 of the Amended Complaint Plaintiff re-alleges the allegations set forth in paragraphs 1 through 13 in the Amended Complaint and in response to paragraph 14 of the Amended Complaint, Secure Computing restates and incorporates by reference its answers to paragraphs 1 through 13 and denies any allegation not expressly admitted.

15. Secure Computing denies the allegations of paragraph 15 of the Amended Complaint.

16. Secure Computing denies the allegations of paragraph 16 of the Amended Complaint.

17. Secure Computing denies the allegations of paragraph 17 of the Amended Complaint.

SECOND CAUSE OF ACTION

(Infringement of the '780 Patent)

18. Secure Computing admits that in paragraph 18 of the Amended Complaint Plaintiff re-alleges the allegations set forth in paragraphs 1 through 17 in the Amended Complaint and in response to paragraph 18 of the Amended Complaint, Secure Computing restates and incorporates by reference its answers to paragraphs 1 through 17 and denies any allegation not expressly admitted.

19. Secure Computing denies the allegations of paragraph 19 of the Amended Complaint.

20. Secure Computing denies the allegations of paragraph 20 of the Amended Complaint.

21. Secure Computing denies the allegations of paragraph 21 of the Amended Complaint.

THIRD CAUSE OF ACTION

(Infringement of the '822 Patent)

22. Secure Computing admits that in paragraph 22 of the Amended Complaint Plaintiff re-alleges the allegations set forth in paragraphs 1 through 21 in the Amended Complaint and in response to paragraph 22 of the Amended Complaint, Secure Computing

restates and incorporates by reference its answers to paragraphs 1 through 21 and denies any allegation not expressly admitted.

23. Secure Computing denies the allegations of paragraph 23 of the Amended Complaint.

24. Secure Computing denies the allegations of paragraph 24 of the Amended Complaint.

25. Secure Computing denies the allegations of paragraph 25 of the Amended Complaint.

PRAYER FOR RELIEF

WHEREFORE, Defendants deny that Plaintiff is entitled to any judgment or relief in Plaintiff's favor, including the relief in paragraphs A through E of the Prayer for Relief in Plaintiff's Amended Complaint.

AFFIRMATIVE DEFENSES

FIRST AFFIRMATIVE DEFENSE

26. Plaintiff fails to state a claim upon which relief can be granted.

SECOND AFFIRMATIVE DEFENSE

27. Plaintiff's claims are barred by the doctrines of waiver, estoppel, and laches.

THIRD AFFIRMATIVE DEFENSE

28. Plaintiff's asserted patents, United States Patent No. 6,092,194 ("the '194 patent"), United States Patent No. 6,804,780 ("the '780 patent"), and United States Patent No. 7,058,822 ("the '822 patent"), are invalid and/or void for failure to satisfy the requirements of patentability contained in 35 U.S.C. Section 101, et seq., including, but not limited to, Sections 102, 103, and for lack of enablement and inadequate written description under 35 U.S.C. section 112, and for failure to disclose best mode.

Exhibit D
Page 5

29. Secure Computing reserves its right to assert additional grounds for the invalidity or unenforceability of the '194 patent, the '780 patent, and the '822 patent if it discovers such grounds during the course of the litigation.

FOURTH AFFIRMATIVE DEFENSE

30. Secure Computing does not infringe, has not induced infringement, and has not contributed to infringement of any valid and enforceable claim of any patent owned by Plaintiff.

FIFTH AFFIRMATIVE DEFENSE

31. Plaintiff's request for damages arising from alleged infringement, whether direct or otherwise, is barred by Plaintiff's failure to plead marking, failure to mark and/or failure to require licensees to mark.

SIXTH AFFIRMATIVE DEFENSE

32. The '194 patent is unenforceable due to Plaintiff's inequitable conduct under 37 C.F.R. § 1.27 and 37 C.F.R § 1.56.

33. Finjan engaged in inequitable conduct by affirmatively misrepresenting and/or failing to disclose material information with an intent to deceive or mislead the PTO. Specifically, Secure Computing's inequitable conduct claims are two-fold: (1) Finjan improperly claimed small-entity status to the PTO; and (2) Finjan made material misrepresentations to the PTO regarding prior art during prosecution.

34. The '194 patent claims the benefit of the filing date of U.S. Patent Application 60/030,639.

35. In U.S. Patent Application 60/030,639, Finjan attached an Appendix describing Finjan's software, SurfinGate, as an embodiment of the alleged invention.

36. In 1998, Finjan entered into an agreement with Cisco Systems, which had over 500 employees, to bundle Finjan's SurfinGate software with Cisco's PIX firewall.

37. On October 27, 1999, Finjan made fee payments to the PTO for the claims in the '194 patent and affirmed that "[a] small entity statement was filed in the prior nonprovisional application and such status is still proper and desired."

38. On information and belief, Finjan knew on October 27, 1999 that small-entity status was no longer proper.

39. On March 27, 2001, in the prosecution of U.S. Patent No. 6,209,103, Finjan paid fees to the PTO as a large entity.

40. Finjan did not notify the PTO in relation to the '194 patent, of its loss of small-entity status until December 12, 2003.

41. Finjan avoided a previous rejection by the PTO examiner during examination based on prior art disclosed in U.S. Patent No. 5,623,600 (Ji). Finjan stated, in the prosecution history, that "Ji teaches gateway detection of viruses attached to executable files, and does not teach hostile Downloadable detection. As is well known in the art, a Downloadable is mobile code that is requested by an ongoing process, downloaded from a source computer to a destination computer for automatic execution. The programs or documents of Ji are not Downloadables."

42. The Ji specification actually teaches that "the apparatus of the present invention could also be included on a FTP server or a world wide web server for scanning files and messages as they are downloaded from the web."

43. On information and belief, Finjan knew that the Ji specification teaches hostile Downloadable detection.

SEVENTH AFFIRMATIVE DEFENSE

44. Plaintiff's claims are barred and/or limited under 28 U.S.C. § 1498.

EIGHTH AFFIRMATIVE DEFENSE

45. Plaintiff's claims that Defendants are inducing infringement and/or contributorily infringing are barred because the underlying alleged direct infringers are licensed and/or released.

NINTH AFFIRMATIVE DEFENSE

46. Plaintiff's claims are barred and/or limited by the doctrine of patent exhaustion.

COUNTERCLAIMS

47. Defendant Secure Computing Corporation ("Secure Computing"), for its Counterclaims against Plaintiff, states:

48. Defendant Secure Computing Corporation is a corporation organized and existing under the laws of the State of Delaware, with its corporate headquarters at 4810 Harwood Road, San Jose, California 95124.

49. On information and belief, Plaintiff Finjan Software Ltd. is a corporation organized and existing under the laws of Israel, with its principal place of business at Hamachsheve St. 1, New Industrial Area, Netanya, 42504, Israel. On information and belief, Plaintiff Finjan Software Ltd. is in the business of developing and distributing network and systems security solutions to organizations.

50. These Counterclaims arise under the Patent Laws of the United States, Title 35, United States Code. The jurisdiction of this Court is founded upon and arises under Title 28, United States Code sections 1331 and 1338(a), and under the Federal Declaratory Judgment Act, Title 28, sections 2201 and 2202. Personal jurisdiction over Plaintiff comports with the United

States Constitution and is proper because Plaintiff has filed suit in this Court against Secure Computing asserting infringement of claims of United States Patent No. 6,092,194, United States Patent No. 6,804,780, and United States Patent No. 7,058,822 and because Plaintiff has and continues to infringe, contributorily infringe and/or induce the infringement of United States Patent No. 7,185,361 and United States Patent No. 6,357,010 in this district. Venue within this judicial district is proper under Title 28, United States Code sections 1391(b), 1391(c) and/or 1400.

COUNT I

DECLARATORY JUDGMENTS
OF INVALIDITY, UNENFORCEABILITY, AND NONINFRINGEMENT

51. This is an action for a declaratory judgment, together with such relief based thereon as may be necessary or proper, pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. Sections 2201 and 2202. There is an actual controversy between Plaintiff and Secure Computing arising under the United States patent laws, Title 35 of the United States Code.

52. This Counterclaim arises under the Patent Laws of the United States, Title 35, United States Code. The jurisdiction of this Court is founded upon and arises under Title 28, United States Code sections 1338(a), and under the Federal Declaratory Judgment Act, Title 28, sections 2201 and 2202. Personal jurisdiction over Plaintiff comports with the United States Constitution and is proper because Plaintiff has filed suit in this Court against Secure Computing asserting infringement of claims of United States Patent No. 6,092,194, United States Patent No. 6,804,780, and United States Patent No. 7,058,822. Venue within this judicial district is proper under Title 28, United States Code sections 1391(b), 1391(c) and/or 1400.

53. Plaintiff alleges that it is the owner of the United States Patent No. 6,092,194, United States Patent No. 6,804,780, and United States Patent No. 7,058,822. Plaintiff contends

that Secure Computing infringes claims of United States Patent No. 6,092,194, United States Patent No. 6,804,780, and United States Patent No. 7,058,822.

54. United States Patent No. 6,092,194 and each claim thereof is invalid, unenforceable and not infringed by Secure Computing. U.S. Patent No. 6,804,780 and each claim thereof is invalid and not infringed by Secure Computing. U.S. Patent No. 7,058,822 and each claim thereof is invalid and not infringed by Secure Computing.

55. Secure Computing has not infringed any valid claims of U.S. Patent No. 6,092,194, either directly, indirectly, contributorily or otherwise, and have not induced any others to infringe said patent. Secure Computing has not infringed any valid claims of U.S. Patent No. 6,804,780, either directly, indirectly, contributorily or otherwise, and have not induced any others to infringe said patent. Secure Computing has not infringed any valid claims of U.S. Patent No. 7,058,822, either directly, indirectly, contributorily or otherwise, and have not induced any others to infringe said patent.

56. With respect to the '194 patent, Finjan engaged in inequitable conduct by affirmatively misrepresenting and/or failing to disclose material information with an intent to deceive or mislead the PTO. Specifically, Secure Computing's inequitable conduct claims are two-fold: (1) Finjan improperly claimed small-entity status to the PTO; and (2) Finjan made material misrepresentations to the PTO regarding prior art during prosecution. Secure Computing incorporates its allegations set forth in paragraphs 32-43 as if fully restated in this counterclaim.

57. Secure Computing therefore seeks a declaration and finding by this Court that United States Patent No. 6,092,194 is invalid and unenforceable and that Secure Computing does

not infringe, directly, indirectly, contributorily or otherwise, and has not induced any others to infringe, any valid claims of United States Patent No. 6,092,194.

58. Secure Computing therefore seeks a declaration and finding by this Court that U.S. Patent No. 6,804,780 is invalid and that Secure Computing does not infringe, directly, indirectly, contributorily or otherwise, and has not induced any others to infringe, any valid claims of U.S. Patent No. 6,804,780.

59. Secure Computing therefore seeks a declaration and finding by this Court that U.S. Patent No. 7,058,822 is invalid and that Secure Computing does not infringe, directly, indirectly, contributorily or otherwise, and has not induced any others to infringe, any valid claims of U.S. Patent No. 7,058,822.

COUNT II

PATENT INFRINGEMENT

60. On February 27, 2007, United States Patent No. 7,185,361 (hereinafter referred to as the "'361 Patent"), entitled "System, Method and Computer Program Product For Authenticating Users Using a Lightweight Directory Access Protocol (LDAP) Directory Server," was duly and legally issued to Thomas D. Ashoff, Steve O. Chew, Jeffrey J. Graham, and Andrew J. Mullican. Secure Computing was assigned all ownership rights to the '361 Patent. A true and correct copy of the '361 Patent is attached as Exhibit A.

61. On March 12, 2002, United States Patent No. 6,357,010 (hereinafter referred to as the "'010 Patent"), entitled "System and Method For Controlling Access To Documents Stored On an Internal Network," was duly and legally issued to Richard R. Viets, David G. Motes, Paula Budig Greve, and Wayne W. Herberg. Secure Computing was assigned all ownership rights to the '010 Patent. A true and correct copy of the '010 Patent is attached as Exhibit B.

62. Plaintiff, Finjan Software Ltd., has directly, indirectly, contributorily, and/or by inducement infringed the '361 Patent in violation of 35 U.S.C. §§ 271(a), (b), (c), and/or (f), literally and/or by the doctrine of equivalents, in this District and elsewhere in the United States, by making, using, selling, offering for sale, and distributing products, including but not limited to Vital Security Internet 1Box™, and will continue to do so unless enjoined by this Court.

63. Finjan's infringement of the '361 Patent has caused injury to Secure Computing, and will continue to do so unless enjoined by this Court, thereby entitling Secure Computing to all remedies available under the Patent Laws of the United States, including 35 U.S.C. § 281-85. The continued infringement will cause irreparable injury and damage to Secure Computing for which Secure Computing has no adequate remedy at law.

64. Finjan has directly, indirectly, contributorily, and/or by inducement infringed the '010 Patent in violation of 35 U.S.C. §§ 271(a), (b), (c), and/or (f), literally and/or by the doctrine of equivalents, in this District and elsewhere in the United States by making, using, selling, offering for sale, and distributing products, including but not limited to its Vital Security™ for Documents (aka Finjan Mirage), and will continue to do so unless enjoined by this Court.

65. Finjan's infringement of the '010 Patent has caused injury to Secure Computing, and will continue to do so unless enjoined by this Court, thereby entitling Secure Computing to all remedies available under the Patent Laws of the United States, including 35 U.S.C. § 281-85. The continued infringement will cause irreparable injury and damage to Secure Computing for which Secure Computing has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG deny that Plaintiff is entitled to any relief for its Amended Complaint and

prays for judgment in Defendants' favor as prayed for in their Answer and Counterclaims and against Plaintiff as follows:

A. That Plaintiff take nothing by its Amended Complaint and its claims against Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be dismissed with prejudice;

B. That Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be found not to infringe, either directly, indirectly, contributorily, or otherwise, and be found not to have induced infringement of any valid claims of United States Patent No. 6,092,194, United States Patent No. 6,804,780, and United States Patent No. 7,058,822;

C. That United States Patent No. 6,092,194 be found invalid and unenforceable;

D. That United States Patent No. 6,804,780 be found invalid;

E. That United States Patent No. 7,058,822 be found invalid;

F. A finding that Plaintiff has directly, indirectly, contributorily, and/or by inducement, literally and/or by the doctrine of equivalents, infringed United States Patent No. 7,185,361 in violation of 35 U.S.C. §§ 271(a), (b), (c), and/or (f);

G. A finding that Plaintiff has directly, indirectly, contributorily, and/or by inducement, literally and/or by the doctrine of equivalents, infringed United States Patent No. 6,357,010 in violation of 35 U.S.C. §§ 271(a), (b), (c), and/or (f);

H. A permanent injunction enjoining Plaintiff and its respective agents, servants, officers, directors, employees, subsidiaries, affiliates, joint venturers, and all persons acting in concert with them, directly or indirectly, from infringing, inducing others to infringe, or contributing to the infringement of United States Patent No. 7,185,361;

I. A permanent injunction enjoining Plaintiff and its respective agents, servants, officers, directors, employees, subsidiaries, affiliates, joint venturers, and all persons acting in concert with them, directly or indirectly, from infringing, inducing others to infringe, or contributing to the infringement of United States Patent No. 6,357,010;

J. An order that Plaintiff account for and pay Secure Computing the damages to which it is entitled as a consequence of patent infringement;

K. An order that Secure Computing be awarded prejudgment interest and its costs, disbursements and attorneys' fees herein in accordance with 35 U.S.C. § 285;

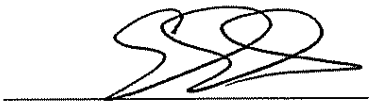
L. For an accounting of Plaintiff's sales, profits, royalties, and damages owing to Secure Computing;

M. That Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be awarded costs, disbursements and attorneys' fees incurred in defending themselves in connection with the Amended Complaint; and

N. That Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG be awarded such other and further relief as the Court deems just, equitable and proper.

DEMAND FOR A JURY TRIAL

Defendants Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG hereby request a trial by jury, pursuant to Rule 38 of the Federal Rules of Civil Procedure, on all issues so triable.



Fredrick L. Cottrell, III (#2555)
cottrell@rlf.com
Gregory E. Stuhlman (#4765)
stuhlman@rlf.com
Richards, Layton & Finger
One Rodney Square
P.O. Box 551
Wilmington, DE 19899
(302) 651-7700

Attorneys for Defendants

OF COUNSEL:

Ronald J. Schutz
Jake M. Holdreith
Christopher A. Seidl
Trevor J. Foster
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Dated: April 20, 2007

CERTIFICATE OF SERVICE

I hereby certify that on April 20, 2007, I electronically filed the foregoing with the Clerk of Court using CM/ECF which will send notification of such filing(s) to the following and which has also been served as noted:

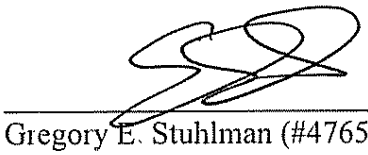
HAND DELIVERY

Philip A. Rovner
Potter Anderson & Corroon LLP
1313 N. Market Street,
Hercules Plaza, 6th Floor
P. O. Box 951
Wilmington, DE 19899-0951

I further certify that on April 20, 2007, the foregoing document was sent to the following non-registered participants in the manner indicated:

FEDERAL EXPRESS

Paul J. Andre
Perkins Coie LLP
101 Jefferson Street
Menlo Park, CA 94025-1114



Gregory E. Stuhlman (#4765)
stuhlman@rlf.com

EXHIBIT A

US007185361B1

(12) **United States Patent**
Ashoff et al.

(10) **Patent No.: US 7,185,361 B1**
(45) **Date of Patent: Feb. 27, 2007**

(54) **SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR AUTHENTICATING USERS USING A LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) DIRECTORY SERVER**

(75) Inventors: **Thomas D. Ashoff**, Mt. Airy, MD (US); **Steve O. Chew**, Pittsburgh, PA (US); **Jeffrey J. Graham**, Olney, MD (US); **Andrew J. Mullican**, Columbia, MD (US)

(73) Assignee: **Secure Computing Corporation**, St. Paul, MN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/495,157

(22) Filed: **Jan. 31, 2000**

(51) **Int. Cl.**
H02H 3/05 (2006.01)

(52) **U.S. Cl.** **726/4**; 713/151; 713/154; 707/1; 726/2; 726/8; 726/11; 726/12; 726/13; 726/14

(58) **Field of Classification Search** 713/201, 713/151–154; 707/1; 726/4, 8, 11–14
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,657,390	A *	8/1997	Elgamal et al	713/151
5,898,830	A *	4/1999	Wesinger, Jr. et al.	713/201
6,047,322	A *	4/2000	Vaid et al	709/224
6,131,120	A *	10/2000	Reid	709/225
6,182,142	B1 *	1/2001	Win et al	709/229
6,212,558	B1 *	4/2001	Antur et al.	709/221
6,233,688	B1 *	5/2001	Montenegro	713/201
6,324,648	B1 *	11/2001	Grantges, Jr.	713/201
2003/0126468	A1 *	7/2003	Markham	713/201

OTHER PUBLICATIONS

Microsoft Corporation, Microsoft Computer Dictionary, Microsoft Press, Third edition, p. 197.*
Definition of application gateway, Webopedia computer dictionary, http://www.webopedia.com/TERM/A/application_gateway.html *
Definition of firewall, Webopedia computer dictionary, http://www.webopedia.com/TERM/firewall.html *
Netegrity, SiteMinder 3.5 Architecture.
How to Securely Manage and Control User Access to E-Commerce Web Sites, Netegrity White Paper, Jul. 1999.
Check Point Account Management Client, Version 1.0, Sep. 1998.
FireWall-1 Architecture and Administration; Chapter 4, pp. 135-154, Sep. 1998.
Howes et al., *The LDAP Application Program Interface*, University of Michigan, Aug. 1995.

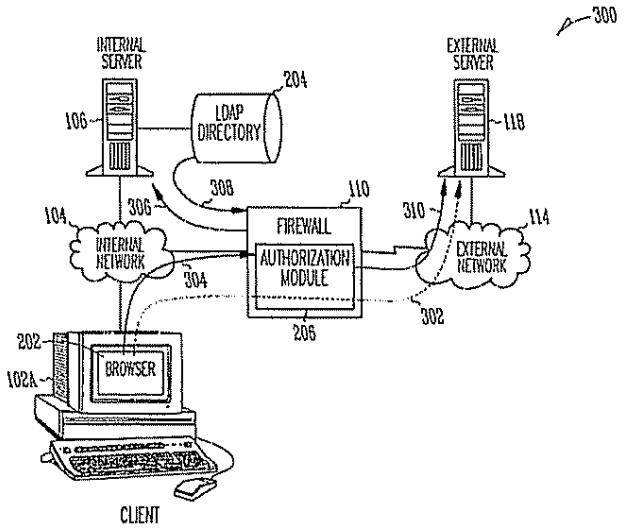
* cited by examiner

Primary Examiner—Taghi T. Arani
(74) *Attorney, Agent, or Firm*—Schwegman, Lundberg, Woessner & Kluth, P.A.

(57) **ABSTRACT**

A system, method and computer program product for providing authentication to a firewall using a lightweight directory access protocol (LDAP) directory server is disclosed. The firewall can be configured through a graphical user interface to implement an authentication scheme. The authentication scheme is based upon a determination of whether at least part of one or more LDAP entries satisfy an authorization filter.

15 Claims, 5 Drawing Sheets



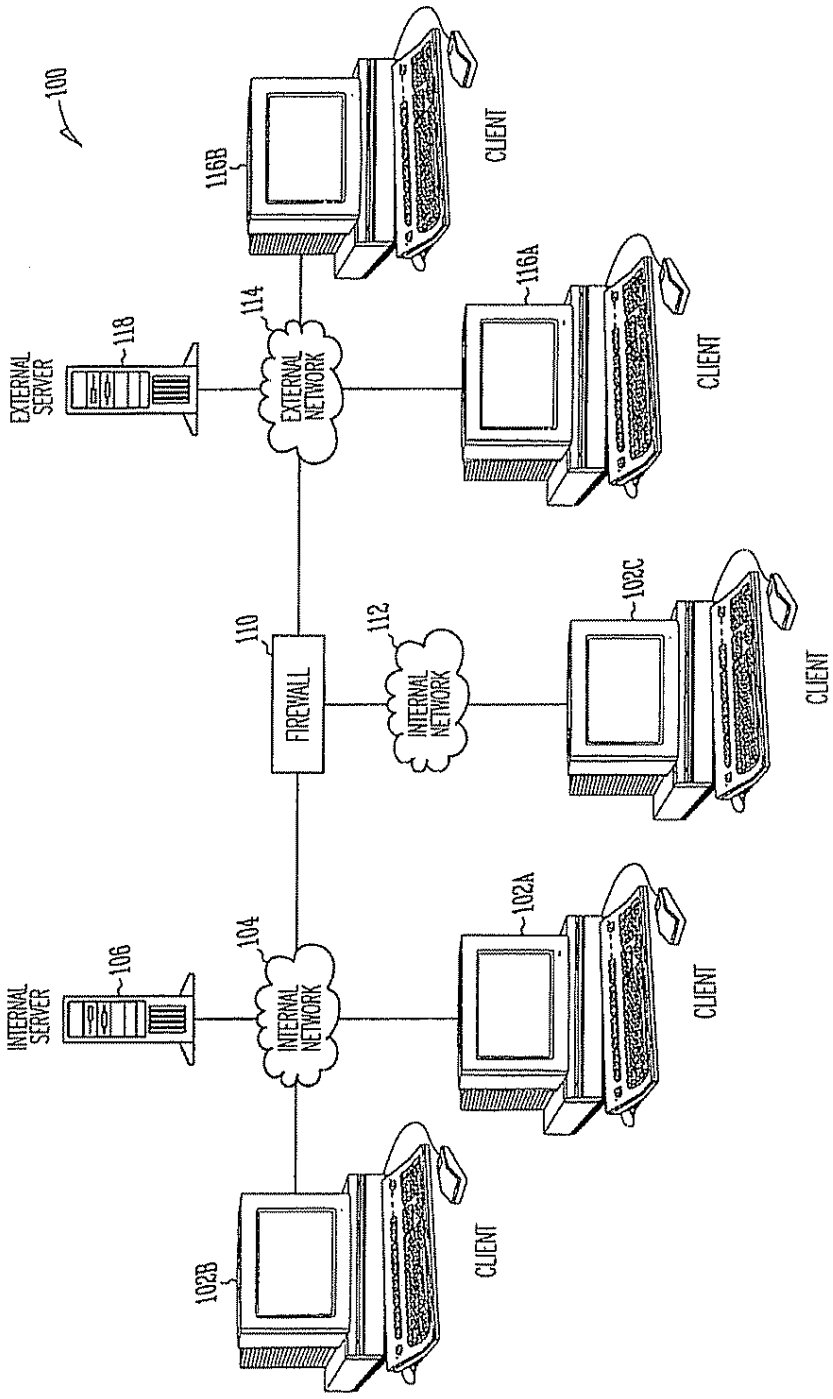


Fig. 1 (Prior Art)

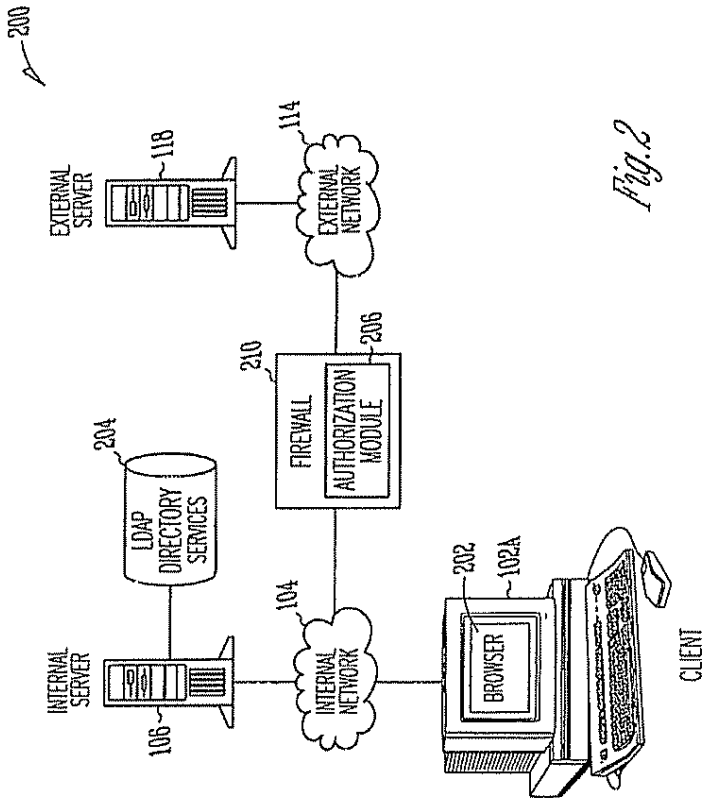

200
EXTERNAL SERVER
118
EXTERNAL NETWORK
114
210
FIREWALL
AUTHORIZATION MODULE
206
204
LDAP DIRECTORY SERVICES
INTERNAL SERVER
106
INTERNAL NETWORK
104
202
BROWSER
102A
CLIENT

Fig. 2

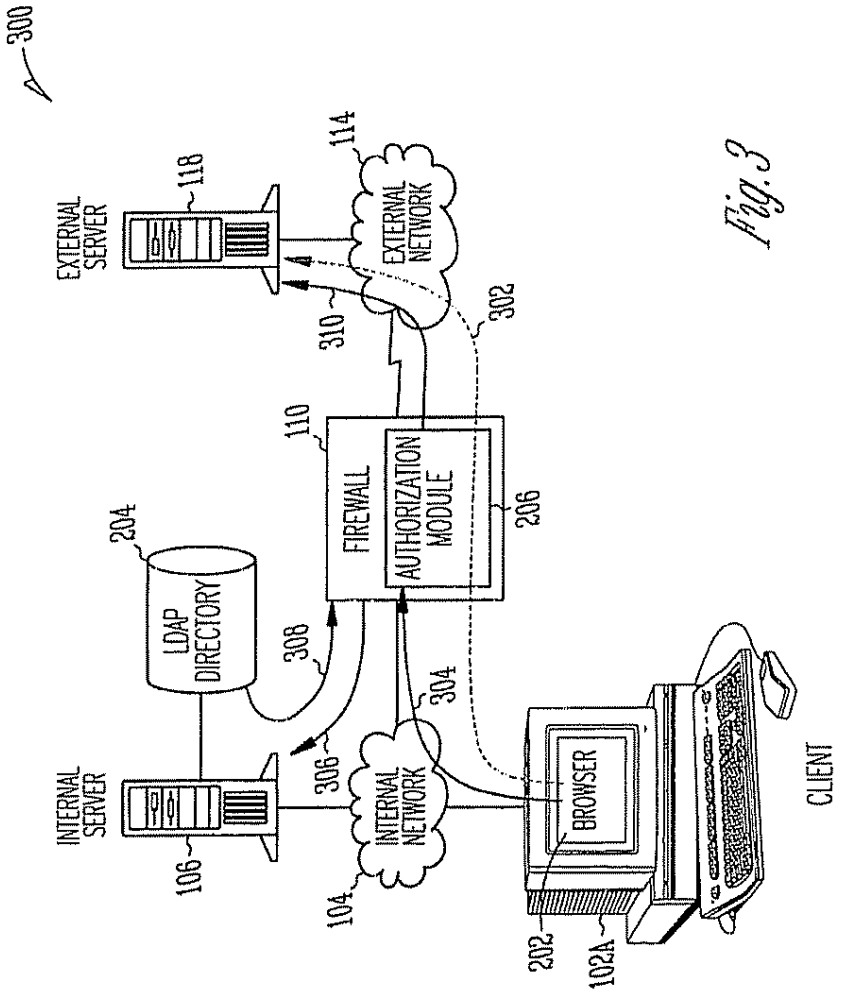

300
EXTERNAL SERVER
118
114
EXTERNAL NETWORK
310
302
110
FIREWALL
AUTHORIZATION MODULE
206
204
LDAP DIRECTORY
308
304
INTERNAL SERVER
106
306
INTERNAL NETWORK
104
BROWSER
202
102A
CLIENT

Fig. 3

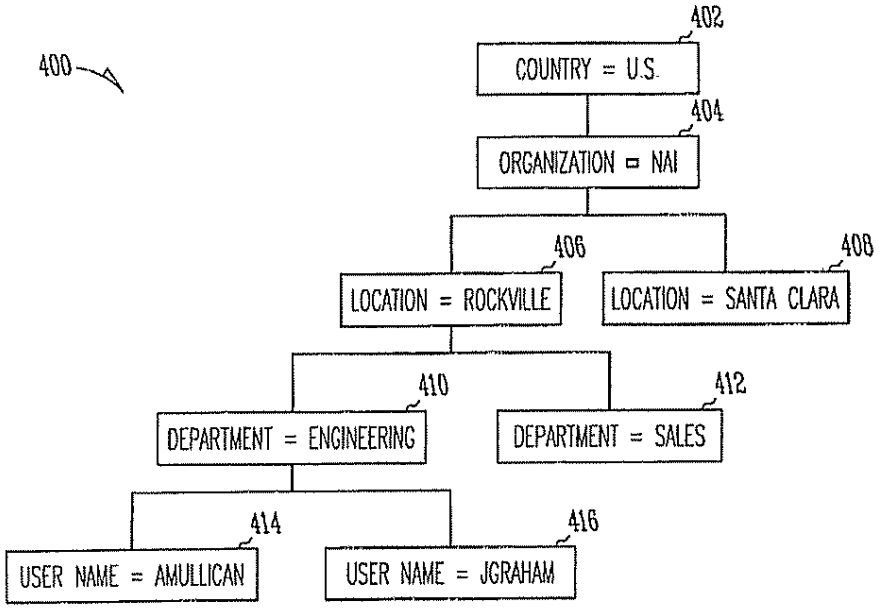

400
402
COUNTRY = U.S.
404
ORGANIZATION = NAI
406
LOCATION = ROCKVILLE
408
LOCATION = SANTA CLARA
410
DEPARTMENT = ENGINEERING
412
DEPARTMENT = SALES
414
USER NAME = AMULLICAN
416
USER NAME = JGRAHAM

Fig. 4

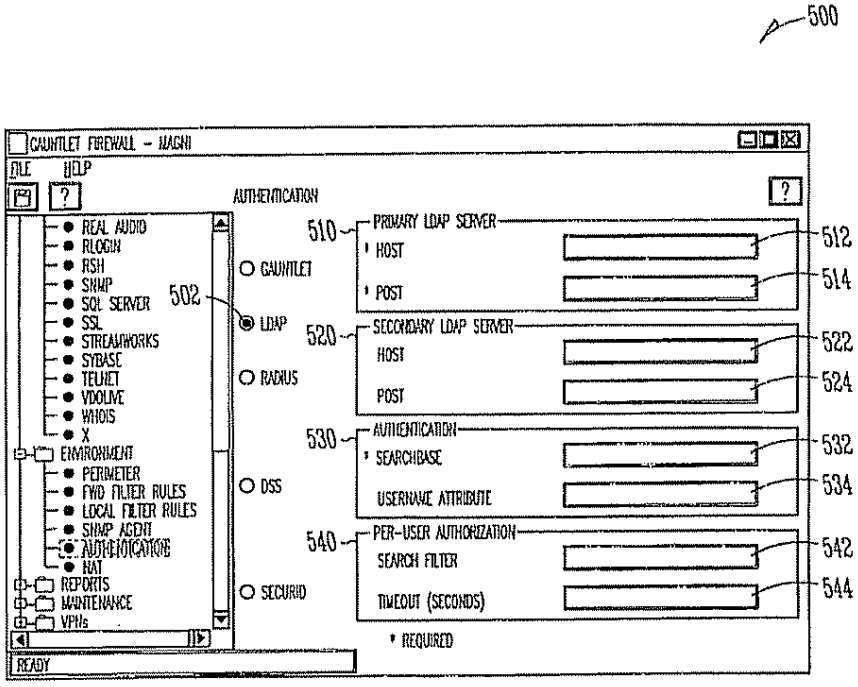

500
GAUNTLET FIREWALL – MAGNI
FILE
HELP
AUTHENTICATION
REAL AUDIO
RLOGIN
RSH
SNMP
SQL SERVER
SSL
STREAMWORKS
SYBASE
TELNET
VDOLIVE
WHOIS
X
ENVIRONMENT
PERIMETER
FWD FILTER RULES
LOCAL FILTER RULES
SNMP AGENT
AUTHENTICATION
NAT
REPORTS
MAINTENANCE
VPNs
502
GAUNTLET
LDAP
RADIUS
DSS
SECURID
510
PRIMARY LDAP SERVER
HOST
POST
512
514
520
SECONDARY LDAP SERVER
HOST
POST
522
524
530
AUTHENTICATION
SEARCHBASE
USERNAME ATTRIBUTE
532
534
540
PER-USER AUTHORIZATION
SEARCH FILTER
TIMEOUT (SECONDS)
542
544
* REQUIRED
READY

Fig. 5

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR AUTHENTICATING USERS USING A LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) DIRECTORY SERVER

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to user authentication mechanisms and more particularly to user authentication mechanisms for firewalls

2. Related Art

Control over access to information technology (IT) resources is a common need today A firewall can be used to protect IT resources behind the firewall. Network firewalls can enforce a site's security policy by controlling the flow of traffic between two or more networks For example, a company might encourage file transfers to the company's network that assist employees, but might discourage file transfers of potentially sensitive company confidential information from the company network to external destinations. Firewalls often are placed between a corporate network and an external network such as, e g., the Internet, or a partnering company's network. Firewalls can also be used to segment parts of a corporate network A firewall system can provide both a perimeter defense to, e g., an internal network, and a control point for monitoring access to and from specific networks such as, e g., an external network.

Firewalls can control access at a network level, an application level, or both. At the network level, a firewall can restrict packet flow based on protocol attributes. For example, the packet's source address, destination address, originating transmission control protocol/user datagram protocol (TCP/UDP) port, destination port, and protocol type can be used for the control decisions At an application level, a firewall can participate in communications between the source and destination applications with the firewall's control decisions being based on details of the conversation and other available information such as, e.g., previous connectivity or user identification Thus, a firewall can authenticate users to control access to and from IT resources behind and before the firewall.

Firewalls can be packaged as system software, combined hardware and software, and, more recently, dedicated hardware appliances (e g, embedded in routers, or easy-to-configure integrated hardware and software packages that can run on dedicated platforms) An example of an application-based firewall is the Gauntlet™ firewall available from Network Associates, Inc.

Firewalls can defend against attacks ranging from, e g, unauthorized access, IP address "spoofing" (i e., a technique by which hackers disguise traffic as coming from a trusted address to gain access to a protected network or resource), buffer overrun attacks, session hijacking, viruses and rogue applets, and rerouting of traffic. However, inherent limitations exist in certain services and protocols that conventional firewalls cannot remedy

Conventionally, when software application programs sought to restrict what a user could do with the programs, the programs required identification of the user. For example, if a user desires access to sensitive corporate financial data in an accounting program, access to the data can be restricted by means of authentication mechanisms such as, e g., a password. The application program therefore requires a list of users and identification information for the user for use in authenticating the user

Early software application programs often included their own integrated authentication mechanisms. Users often use a variety of software application programs, each possibly having its own authentication mechanism. Users find it cumbersome to remember different passwords associated with each of the multiple software application programs

IT resources used by companies today can include access to multiple software application programs and Internet based applications. For example, employees at a given company can use e-mail and groupware applications, and other office automation programs including, e g, to spreadsheets, word-processors and presentation programs As every application program conventionally has its own authentication mechanism, a separate database is initialized and updated for each application.

Authentication mechanisms can use a query to a database known as a directory that can store information about users. A directory is similar to a database in that one can store information in a directory and later retrieve the information from it. However, a directory is specialized in that a directory is typically designed for reading more than writing. A directory offers a static view of the information and allows simple updates without transactions. Thus, while a database is typically written to and read from frequently, a directory by comparison is primarily read from and is infrequently updated.

A directory service includes all the functions of a directory and adds a network protocol that can be used to access the directory. Standardization is desirable in implementing a directory service.

An early standard for directory service was the directory access protocol (DAP), which originated in the European standards organization. DAP although specifying a vast, feature-rich protocol for storing and encoding directory information, was unwieldy in size.

Today, a new protocol, lightweight directory access protocol (LDAP), is gaining wide acceptance in business The LDAP standard defines an information model for a directory, a namespace for defining how directory information is referenced and organized, and a network protocol for accessing information in the directory. LDAP can also include an application programming interface (API) The LDAP protocol mandates how client and server computers can communicate with a LDAP directory. However, LDAP does not mandate how data should be stored More and more companies today use an LDAP directory server to store a database of employees The LDAP directory generally can store an employee name, phone number, address and other information about the employee, and a password for modifying the employee's information.

Firewalls also maintain a database of users and are operative to prompt users for an identifying user identifier and password These conventional firewalls require that employee names and passwords be entered into a firewall authentication database. Maintenance of the firewall authentication database is especially burdensome where there are a large number of employees that are frequently leaving or joining a company or when a company has a large number of firewalls. Accordingly, what is needed is a mechanism for reducing this administrative burden More specifically, what is needed is a mechanism for leveraging an existing LDAP directory server as part of a firewall's authentication process In this manner, an existing LDAP directory server can be used as a central directory that stores the data used by all applications.

SUMMARY OF THE INVENTION

A system, method and computer program product for enabling the authentication of users to a firewall using a lightweight directory access protocol (LDAP) directory server is provided by the present invention. The firewall can be configured through a graphical user interface to implement an authentication scheme. The authentication scheme is based upon a determination of whether information contained in one or more LDAP entries satisfy an authorization filter. It is a feature of the present invention that the authentication scheme can be configured independently of specifically stated field requirements or schema of the firewall. In accordance with the present invention, the authentication scheme can be flexibly specified to interact with a LDAP directory that has been uniquely developed for a company's internal needs. The company's investment in its existing administrative infrastructure can therefore be leveraged to a greater degree.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other features and advantages of the invention will be apparent from the following, more particular description of a preferred embodiment of the invention, as illustrated in the accompanying drawings.

FIG. **1** illustrates a communications network including a firewall.

FIG. **2** illustrates a communications network including a lightweight directory access protocol (LDAP) directory server and an authorization module within a firewall.

FIG. **3** illustrates the authentication of a client user through a firewall.

FIG. **4** illustrates an example embodiment of an LDAP directory tree.

FIG. **5** illustrates an embodiment of a graphical user interface for configuring the LDAP authentication feature.

DETAILED DESCRIPTION OF THE INVENTION

A preferred embodiment of the invention is discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the invention.

FIG. **1** illustrates an example embodiment of a communications network **100** including client computers **102***a* and **102***b* coupled via an internal network **104** to an internal server computer **106** and a firewall **110**. Communications network **100** also includes a client computer **102***c* coupled via an internal network **112** to firewall **110**. Finally, communications network **100** includes client computers **116***a* and **116***b* coupled via an external network **114** to an external server computer **118** and firewall **110**. External network **114** can represent, e.g., the Global Internet, or a partnering company's network.

Network firewall **110** can enforce a business' security policy by controlling the flow of traffic between two or more networks such as, e.g., internal networks **104** and **112** and external network **114**. In general, firewall **110** serves to isolate internal networks **104** and **112** from one another and also from external network **114**.

As illustrated in FIG. **1**, firewall **110** can be used to segment parts of a corporate network. For example, firewall **110** can be used to control information flow between a corporation's internal networks **104**, **112**. Firewall **110** can also provide a perimeter defense between an internal network **104**, **112** and an external network **114**.

FIG. **2** illustrates an example embodiment of a communications network **200** that includes client computer **102***a* coupled via internal network **104** to internal server **106** and to firewall **210**. Firewall **210** is also coupled via external network **114** to external server **118**.

As shown, client computer **102***a* includes a browser **202**. Browser **202** can in one embodiment be an Internet browser that provides a graphical user interface to network resources. Browser **202** is generally operative to parse and make requests to network resources such as, e.g., external server **118**, and present the results of the request to a client user viewing client computer **102***a*.

Internal server **106** is shown including a lightweight directory access protocol (LDAP) directory **204**, which can be configured to store employee information. For example, a human resources database could be stored as an LDAP directory having a directory structure such as that illustrated in FIG. **4**. As illustrated, LDAP directory tree **400** includes country **402** set in this example to US, organization **404** set to NAI, location **406** set to Rockville and location **408** set to Santa Clara, department **410** set to engineering and department **412** set to sales, and username **414** set to amullican and username **416** set to jgraham.

External server **118** can include an Internet server application. In one embodiment, the Internet server application supports file transfer protocol (FTP) communication. As would be apparent to those skilled in the relevant art, other types of server applications can be included on external server **118** including, e.g., databases, and electronic mail.

Firewall **210** is shown including an authorization module **206**. Authorization module **206** is used to authenticate a client user (e.g., client computer **102***a*) to determine if the client user's communication is authorized to pass through firewall **210**. Conventional firewalls **110** included their own database having a list of users and passwords, to enable authentication through firewall **110**.

In accordance with the present invention, firewall **210** does not authenticate users using its own database. Rather, firewall **210** authenticates users using information contained within LDAP directory **204**. As will be described in greater detail below, firewall **210** can authenticate users through an authentication scheme that can be based upon the unique composition of an organization's LDAP directory **204**.

It is a feature of the present invention that the authentication scheme of the present invention can operate independently of specifically stated field requirements or schema of the firewall **210**. In other words, an organization's LDAP directory **204** need not be modified to conform to a schema imposed by the firewall **210**. Moreover, resistance to such a modification will not result in the maintenance of multiple directories.

In accordance with the present invention, the authentication scheme can be flexibly specified to interact with an existing LDAP directory that has been uniquely developed for a organization's internal needs. This framework enables a firewall administrator to seamlessly integrate a firewall product into an existing administrative infrastructure. The organization's investment in the existing administrative infrastructure can therefore be leveraged to a greater degree.

FIG. **3** illustrates the authentication process that is implemented by firewall **210**. In the illustrated example, firewall **210** authenticates a client user at client computer **102***a* running a browser **202** that is attempting to access an

application or resource on external server **118**. This access path is illustrated by path **302**.

This authentication process begins when client computer **102***a* initiates a network resource request **304** from browser **202**. The network resource request **304** is intercepted by firewall **210**. Authorization module **206** within firewall **210** challenges the client user to identify himself or herself. A challenge could in one embodiment include a request for entry of a username and password. Upon receipt of the identification information, authorization module **206** searches an authentication database (not shown) to identify an authentication method (e.g., LDAP authentication). If no entry in the authentication database is found for the client user, then a default authentication method can be used. In the LDAP authentication process, authorization module **206** binds to LDAP directory **204** and uses the userPassword attribute for authentication.

After authorization module **206** authenticates the client user, authorization module **206** then determines whether the client user is authorized to have his access request fulfilled. The LDAP authorization process is illustrated as communications **306** and **308**. Communications **306** and **308** are facilitated using the LDAP protocol and may utilize the secure sockets layer.

If per-user authorization is configured, authorization module **206** determines whether one or more attributes of the client user's LDAP entry satisfies an authorization filter. If the one or more attributes of the client user's LDAP entry does not satisfy the authorization filter, then authorization module **206** determines that the authorization fails. If the authorization filter is satisfied, then the client user's network resource request is allowed through firewall **210**. This allowed connection is illustrated in FIG. **3** as path **310**.

To support per-user authorization, an administrator configures an authorization filter to use when authenticating users. One or more attributes in the client user's LDAP directory entry and associated values can be selected for the authorization filter. Once configured, authorization module **206** can verify that the LDAP entry used in the bind call satisfies the authorization filter before allowing the user access to/through the firewall.

FIG. **5** illustrates an example embodiment of a graphical user interface (GUI) **500** of a firewall systems administrator application screen. As shown by a selected radio button, LDAP authentication **502** has been selected. GUI **500** includes a primary LDAP server settings area **510**, a secondary LDAP server settings area **520**, an authentication settings area **530**, and a per-user authorization settings area **540**.

The primary LDAP server settings area **510** includes a host field **512** and a port field **514**. The host field **512** can be used to enter an IP address or host name of a primary LDAP server. The port field **514** can be used to enter the port to be used on the primary LDAP server.

The secondary LDAP server settings area **520** also includes a host field **522** and a port field **524**. The host field **522** can be used to enter an IP address or host name of a secondary LDAP server. The port field **524** is used to enter the port to be used on the secondary LDAP server. Fields **522**, **524** can be left blank if no secondary LDAP server is being used.

The authentication settings area **530**, can include searchbase field **532** and a username attribute field **534**. The searchbase field **532** can be used to indicate the top of the directory tree **400** such as, e.g., country **402**, organization **404**, location **406**, and department **410**, so that a lookup can be within that portion of the directory tree. For example, a set of attribute pairs such as, e.g., o=NAI, c=US to append to all requests to the LDAP server can be entered. The username attribute field **534** can include a default username attribute such as, e.g., uid. The username attribute field **534** can be used in performing per-user authorization.

The per-user authorization settings area **540** includes a search filter field **542** and a timeout field **544**. The timeout field **544** can include a default value such as, e.g., 60 seconds. For example, timeout field **544** can be used to limit the amount of time the authorization filter query can take. If the time is exceeded, the authorization fails.

The search filter field **542** is used by firewall **210** in identifying the appropriate fields that are the subject of the LDAP directory authentication query. Upon receipt of a response from the LDAP directory **204**, firewall **210** can then determine whether the client user is authorized to authenticate through the firewall **210**.

In general, the authorization filter can contain any LDAP-valid combination of attributes and values, including object classes. At its simplest, the authorization filter specifies a single attribute and value pair. For example, the search filter field **542** can be used to enter a search filter expression such as "objectclass=gauntletUser."

Consider another example where LDAP directory **204** is configured by the company to include a field that would provide an access code level for each user. For example a "1" could correspond to only e-mail access, while a 5 could mean full access to all Internet services including world wide web browsing. In this environment, an authorization filter can be specified as "(&(objectclass=gUser)(status>=5))".

It should be noted that the authorization process need not be based on per-user authorization. In another embodiment, the authorization process can be based on a per-service authorization. In this embodiment, the per-service authorization can include an authorization for protocol services. Examples of protocol services include FTP, simple mail transport protocol (SMTP) e-mail, hypertext transport protocol (HTTP), etc. The per-service authorization can also be based on LDAP directory information. For example, authorization module **206** can use group memberships to determine whether a client user can use HTTP through firewall **210**. To satisfy this authorization process, the authenticated user must be a member of the "web-users" group in the LDAP directory.

In one embodiment, the per-service authorization process uses the standard groupOfNames and groupOfUniqueNames object classes for authorization decisions. In general, a mechanism can be included that supports the specification of arbitrary group names for each service to be controlled. Control can then be based on a per-proxy basis or a per-policy basis.

Specification of per-service authorization criteria can also be implemented using the search filter field **542**. In general, a different search (or authorization) filter can be provided for each service. For example, a search filter field can be included in GUI **500** to determine whether, e.g., a user is authorized to perform a file transfer, to send e-mail, or to access the world wide web. A search filter field can also be included in GUI **500** to determine whether, e.g., a user is a member of a particular group such as, e.g., engineering department **410**, and if so, then particular services can be authorized based on being part of that group.

As noted, it is a feature of the present invention that firewall **210** can support arbitrary LDAP directory schema. Accordingly, firewall **210** does not require additional firewall-specific object classes or attributes in the directory

Customers can populate the LDAP directories with whatever data they require. This authentication environment can be flexibly applied across multiple organizations each having their own sets of directory information. Indeed, the concepts of the present invention can be used to implement an authorization filter that relies on portions of information that are stored in distinct LDAP directories. This distributed authentication scheme enables an organization to implement segmented management of the user database.

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1. A system for authorizing client access to a network resource, comprising:

a server having at least one directory that can be accessed using a network protocol, said at least one directory being configured to store information concerning an entity's organization; and

a firewall that is configured to intercept network resource requests from a plurality of client users on an internal network, said firewall being operative to authorize a network resource request based upon a comparison of the contents of at least part of one or more entries in said at least one directory to an authorization filter, wherein said authorization filter is generated based on a directory schema that is predefined by said entity.

2. The system of claim 1, wherein said at least one directory is a lightweight directory access protocol directory.

3. The system of claim 1, wherein said authorization filter is specified using a graphical user interface.

4. The system of claim 1, wherein said authorization filter implements a per-user authentication scheme.

5. The system of claim 1, wherein said authorization filter implements a per-service authentication scheme.

6. The system of claim 1, wherein said firewall and said directory communicate using secure socket layer communication.

7. The system of claim 1, wherein said firewall is configured to query multiple directories.

8. An authentication method at a firewall, comprising the steps of:

(a) receiving a network resource request from a client user at an internal network;

(b) querying, using a network protocol, at least one directory that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter that is generated based on a directory schema that is predefined by said entity;

(c) determining, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter; and

(d) permitting said network resource request through said firewall if said authorization filter is satisfied.

9. The method of claim 8, wherein step (b) comprises the step of querying said at least one directory using a lightweight directory access protocol.

10. The method of claim 8, further comprising the step of specifying an authorization filter using a graphical user interface.

11. The method of claim 10, wherein said specifying step comprises the step of specifying an authorization filter that implements a per-user authentication scheme.

12. The method of claim 10, wherein said specifying step comprises the step of specifying an authorization filter that implements a per-service authentication scheme.

13. The method of claim 8, wherein step (b) comprises the step of querying said directory using secure socket layer communication.

14. The method of claim 8, wherein step (b) comprises the step of querying multiple directories.

15. A computer program product for enabling a processor in a computer system to implement an authentication process, said computer program product comprising:

a computer usable medium having computer readable program code embodied in said medium for causing a program to execute on the computer system, said computer readable program code comprising:

first computer readable program code for enabling the computer system to receive a network resource request from a client user at an internal network;

second computer readable program code for enabling the computer system to query, using a network protocol, at least one directory that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter that is generated based on a directory schema that is predefined by said entity;

third computer readable program code for enabling the computer system to determine, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter; and

fourth computer readable program code for enabling the computer system to permit said network resource request through a firewall if said authorization filter is satisfied.

* * * * *

EXHIBIT B

US006357010B1

(12) **United States Patent**
Viets et al.

(10) **Patent No.: US 6,357,010 B1**
(45) **Date of Patent: Mar. 12, 2002**

(54) **SYSTEM AND METHOD FOR CONTROLLING ACCESS TO DOCUMENTS STORED ON AN INTERNAL NETWORK**

(75) Inventors: **Richard R. Viets**, Naples; **David G. Motes**, Bonita Springs, both of FL (US); **Paula Budig Greve**, St. Anthony; **Wayne W. Herberg**, Rush City, both of MN (US)

(73) Assignee: **Secure Computing Corporation**, Roseville, MN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No : **09/024,576**

(22) Filed: **Feb. 17, 1998**

(51) **Int. Cl.**[7] **G06F 12/14**; G06F 15/173; H04L 12/00; H04L 9/00

(52) **U.S. Cl.** **713/201**; 709/225; 713/200

(58) **Field of Search** 713/201, 200; 709/225

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,956,615	A		5/1976	Anderson et al.	235/61.7 B
4,177,510	A		12/1979	Appell et al	364/200
4,584,639	A		4/1986	Hardy	364/200
4,621,321	A		11/1986	Boebert et al.	364/200
4,701,840	A		10/1987	Boebert et al.	364/200
4,713,753	A		12/1987	Boebert et al.	364/200
4,914,568	A		4/1990	Kodosky et al	364/200
5,124,984	A		6/1992	Engle	370/94.1
5,179,658	A	*	1/1993	Izawa	345/508
5,204,812	A	*	4/1993	Kasiraj et al.	707/9
5,272,754	A		12/1993	Boebert	380/25
5,276,735	A		1/1994	Boebert et al	380/21
5,311,593	A		5/1994	Carmi	380/23
5,329,623	A		7/1994	Smith et al.	395/275
5,455,953	A	*	10/1995	Russell	710/266
5,544,321	A	*	8/1996	Theimer et al.	714/9
5,566,170	A		10/1996	Bakke et al	370/60
5,586,260	A		12/1996	Hu	395/200.2
5,606,668	A		2/1997	Shwed	395/200.11
5,619,648	A		4/1997	Canale et al	395/200.01

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

EP	0697662 A1	2/1996	G06F/12/14
EP	0 743 777 A2	11/1996	H04L/29/06
EP	0811939 A2	12/1997	G06F/17/30
WO	97/13340	4/1997	H04L/9/00
WO	97/16911	5/1997	H04L/29/06
WO	97/26731	7/1997	H04L/9/00

OTHER PUBLICATIONS

Yialelis et al. "Role–Based Security for Distributed Object Systems", IEEE Proceeding, 1996, pp. 80–85.*

Sandhu et al "Role–Based Access Control Models", IEEE Computer, Feb 1996, pp. 38–47.*

Tari et al. "Role–Based Access Control For Intranet Security", IEEE Internet Computing, 1997, pp. 24–34.*

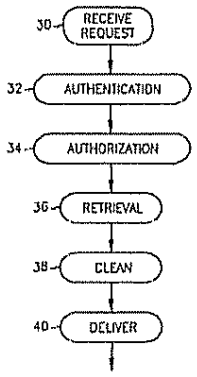
(List continued on next page.)

Primary Examiner—Thomas Lee
Assistant Examiner—Tanh Q. Nguyen
(74) *Attorney, Agent, or Firm*—Schwegman, Lundberg, Woesnner & Kluth, P.A.

(57) **ABSTRACT**

A system and method of limiting access from an external network to documents stored on an internal network. A client list is built in which each client is assigned to one or more roles. Each role has access to one or more documents as defined on a document list. A request from an external network is reviewed and, if possible, the request is associated with a client on the client list. The requested document is then compared to the document list associated with the client's role and, if the requested document is in the list of documents available to a client in the client's role, the requested document is fetched, cleaned and sent to the client.

37 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

5,623,601	A	4/1997	Vu	395/187.01
5,636,371	A	6/1997	Yu	395/500
5,673,322	A	9/1997	Pepe et al.	380/49
5,684,951	A	11/1997	Goldman et al.	395/188.01
5,689,566	A	11/1997	Nguyen	380/25
5,701,137	A *	12/1997	Kiernan et al.	345/340
5,708,780	A	1/1998	Levergood et al.	395/200.12
5,784,566	A *	7/1998	Viavant et al.	709/229
5,802,299	A *	9/1998	Logan et al.	709/218
5,819,271	A *	10/1998	Mahoney et al.	707/9
5,826,029	A *	10/1998	Gore, Jr. et al.	709/227
5,864,683	A *	1/1999	Boebert et al.	709/249
5,864,871	A *	1/1999	Kitain et al.	707/104
5,870,544	A *	2/1999	Curtis	713/201
5,884,033	A *	3/1999	Duvall et al.	709/206
5,884,312	A *	3/1999	Dustan et al.	707/10
5,892,905	A *	4/1999	Brandt et al.	713/201
5,903,732	A *	5/1999	Reed et al.	709/229
5,911,143	A *	6/1999	Deinhart et al.	707/103
5,913,024	A *	6/1999	Green et al.	713/200
5,915,087	A *	6/1999	Hammond et al.	713/201
5,918,013	A *	6/1999	Mighdoll et al.	709/217
5,933,600	A *	8/1999	Shieh et al.	709/219
5,950,195	A *	9/1999	Stockwell et al.	707/4
5,961,601	A *	10/1999	Iyengar	709/229
5,987,611	A *	11/1999	Freund	713/201
6,023,765	A *	2/2000	Kuhn	713/200
6,055,637	A *	4/2000	Hudson et al.	713/201
6,088,679	A *	7/2000	Barkley	705/8

OTHER PUBLICATIONS

International Search Report, PCT Application No. PCT/US 95/12681, 8 p. (mailed Apr. 9, 1996)

Ancilotti, P., et al., "Language Features for Access Control", *IEEE Transactions on Software Engineering, SE–9*, 16–25 (Jan. 1983).

Atkinson, R., "IP Authentication Header", Network Working Group, Request For Comment No. 1826, http//ds.internic.net/rfc/rfc1826.txt, 9 p. (Aug. 1995).

Atkinson, R., "IP Encapsulating Security Payload (ESP)", Network Working Group, Request For Comment No. 1827, http//ds.internic.net/rfc/rfc1827.txt, 12 p. (Aug. 1995).

Atkinson, R., "Security Architecture for the Internet Protocol", Network Working Group, Reqest for Comment No. 1825, http//ds.internic.net/rfc/rfc1825.txt, 21 p. (Aug. 1995)

Baclace, P.E., "Competitive Agents for Information Filtering", *Communications of the ACM*, 35, 50 (Dec. 1992).

Badger, L., et al., "Practical Domain and Type Enforcement for UNIX", *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, p. 66–77 (May 1995).

Belkin, N.J., et al., "Information Filtering and Information Retrieval: Two Sides of the Same Coin?", *Communications of the ACM*, 35, 29–38 (Dec. 1992)

Bellovin, S.M., et al., "Network Firewalls", *IEEE Communications Magazine*, 32, 50–57 (Sep. 1994).

Bevier, W.R., et al., "Connection Policies and Controlled Interference", *Proceedings of the Eighth IEEE Computer Security Foundations Workshop*, Kenmare, Ireland, p. 167–176 (Jun. 13–15, 1995).

Bowen, T.F., et al., "The Datacycle Architecture", *Communications of the ACM*, 35, 71–81 (Dec. 1992).

Bryan, J., "Firewalls For Sale", *BYTE*, 99–100, 102, 104–105 (Apr. 1995).

Cobb, S., "Establishing Firewall Policy", *IEEE*, 198–205 (1996)

Foltz, P.W., et al., "Personalized Information Delivery: An Analysis of Information Filtering Methods", *Communications of the ACM*, 35, 51–60 (Dec. 1992).

Gassman, B., "Internet Security, and Firewalls Protection on the Internet", *IEEE*, 93–107 (1996).

Goldberg, D., et al., "Using Collaborative Filtering to Weave an Information Tapestry", *Communications of the ACM*, 35, 61–70 (DEC. 1992).

Grampp, F.T. "UNIX Operating System Security", *AT& T Bell Laboratories Technical Journal*, 63, 1649–1672 (Oct 1984).

Greenwald, M., et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF", *IEEE*, 79–92 (1996).

Haigh, J.T., et al., "Extending the Noninterference Version of MLS for SAT", Proceedings of the 1986 IEEE Symposium on Security and Privacy, Oakland, CA, p. 232–239 (Apr. 7–9, 1986).

Karn, P., et al., "The ESP DES–CBC Transform", Network Working Group, Request for Comment No. 1829, http//ds.internic.net/rfc/rfc1829.txt, 9 p. (Aug. 1995).

Kent, S.T., "Internet Privacy Enhanced Mail", *Communications of the ACM*, 36, 48–60 (Aug. 1993).

Lampson, B.W., et al., "Dynamic Protection Structures", *AFIPS Conference Proceedings*, 35, 1969 Fall Joint Computer Conference, Las Vegas, NV, 27–38 (Nov. 18–20, 1969).

Lee, K.C., et al., "A Framework for Controlling Cooperative Agents", *Computer*, 8–16 (Jul. 1993).

Lodin, S.W., et al., "Firewalls Fend Off Invasions from the Net", *IEEE Spectrum*, 26–34 (Feb. 1998).

Loeb, S., "Architecting Personalized Delivery of Multimedia Information", *Communications of the ACM*, 35, 39–48 (1992).

Loeb, S., et al., "Information Filtering", *Communications of the ACM*, 35, 26–28 (Dec. 1992).

Merenbloom, P., "Network 'Fire Walls' Safeguard LAN Data from Outside Intrusion", *Infoworld*, p. 69 & addnl page (Jul. 25, 1994).

Metzger, P., et al., "IP Authentication using Keyed MD5", Network Working Group, Request for Comments No. 1828, http//ds.internic.net/rfc/rfc1828.txt, 5 p. (Aug. 1995).

Obraczka, K., et al., "Internet Resource Discovery Services", *Computer*, 8–22 (Sep. 1993).

Peterson, L.L., et al., In: *Computer Networks*, Morgan Kaufmann Publishers, Inc., San Francisco, CA, p. 218–221, 284–286 (1996).

Press, L., "The Net: Progress and Opportunity", *Communications of the ACM*, 35, 21–25 (Dec. 1992)

Schroeder, M.D., et al., "A Hardware Architecture for Implementing Protection Rings", *Communications of the ACM*, 15, 157–170 (Mar. 1972).

Schwartz, M.F., "Internet Resource Discovery at the University of Colorado", *Computer*, 25–35 (Sep. 1993).

Smith, R.E., "Constructing a High Assurance Mail Guard", Secure Computing Corporation (Appeared in the Proceedings of the National Computer Security Conference), 7 p. (1994).

Smith, R.E., "Sidewinder: Defense in Depth Using Type Enforcement", *International Journal of Network Management*, p. 219–229 (Jul.–Aug. 1995).

Stadnyk, I., et al., "Modeling User's Interests in Information Filters", *Communications of the ACM*, 35, 49–50 (Dec. 1992).

Stempel, S., "IpAccess—An Internet Service Access System for Firewall Installations", *IEEE*, 31–41 (1995).
Stevens, C., "Automating the Creation of Information Filters", *Communications of the ACM*, 35, 48 (Dec. 1992).
Thomsen, D., "Type Enforcement: The New Security Model", *SPIE*, 2617, 143–150 (1995).
Warrier, U.S., et al., "A Platform for Heterogeneous Interconnection Network Management", *IEEE Journal on Selected Areas in Communications*, 8, 119–126 (Jan. 1990).
White, L.J., et al., "A Firewall Concept for Both Control–Flow and Data–Flow in Regression Integration Testing", *IEEE*, 262–271 (1992).
Wolfe, A., "Honeywell Builds Hardware for Computer Security", *Electronics*, 14–15 (Sep. 2, 1985)

Boebert, W.E., et al., "Secure Ada Target: Issues, System Design, and Verification", *Proceedings of the Symposium on Security and Privacy*, Oakland, California, Oakland, California, pp. 59–66, (1985).

Boebert, W.E., et al., "Secure Computing: The Secure Ada Target Approach", *Sci. Honeyweller*, 6(2), 17 pages, (1985).

Kahan, J., "A capability based authorization model for the world–Wide Web", *Computer Networks and ISDN Systems*, pp. 1055–1064, (1995)

Vinter, S.T., et al., "Extended Discretionary Access Controls", *IEEE*, pp 39–49, (1988).

* cited by examiner

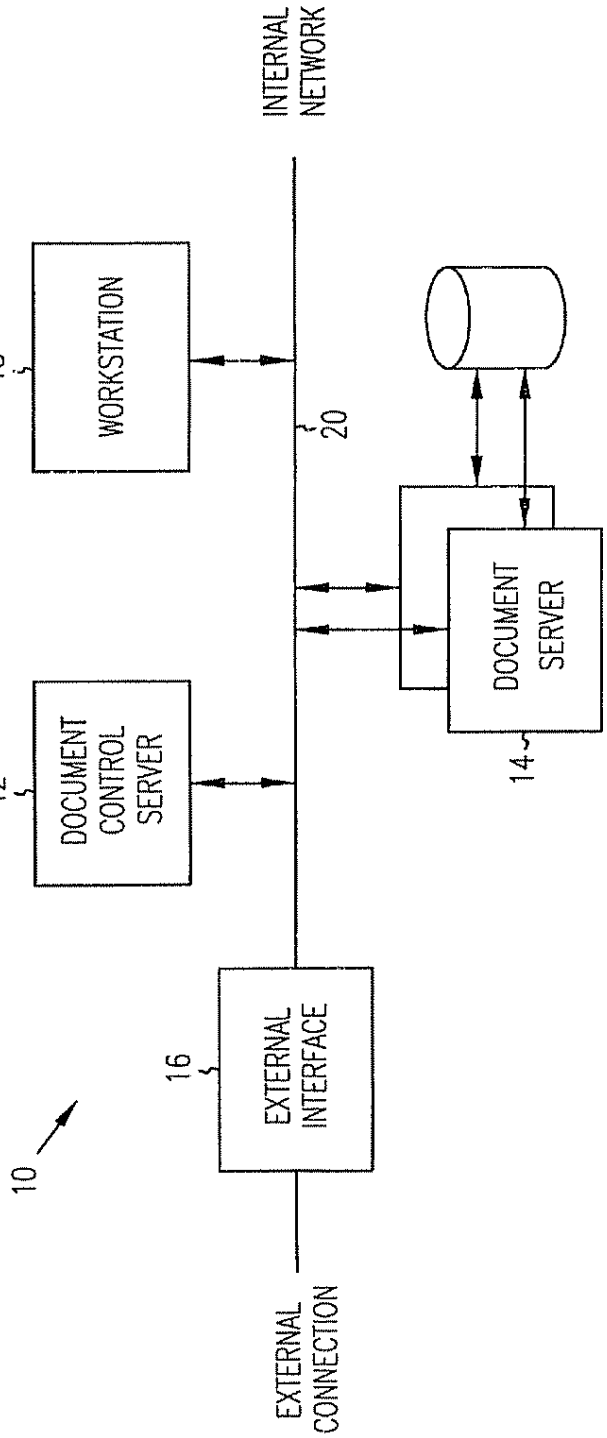

INTERNAL NETWORK
WORKSTATION
18
20
DOCUMENT SERVER
14
DOCUMENT CONTROL SERVER
12
EXTERNAL INTERFACE
16
10
EXTERNAL CONNECTION

FIG. 1

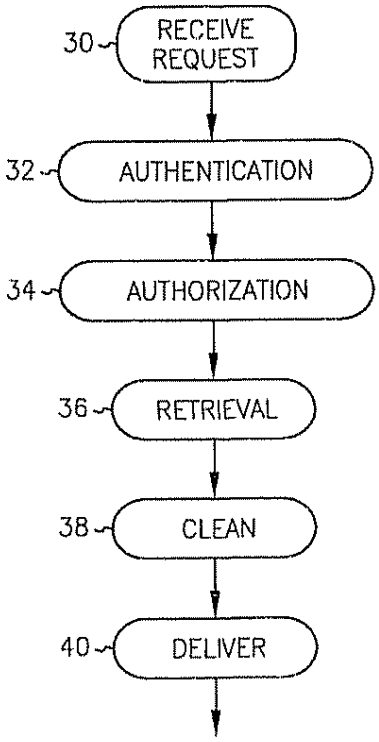

30
RECEIVE REQUEST
32
AUTHENTICATION
34
AUTHORIZATION
36
RETRIEVAL
38
CLEAN
40
DELIVER

FIG. 2

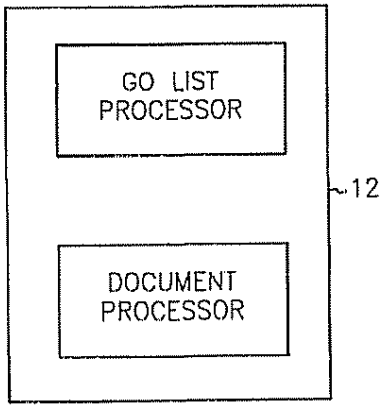

GO LIST PROCESSOR
12
DOCUMENT PROCESSOR

FIG. 3

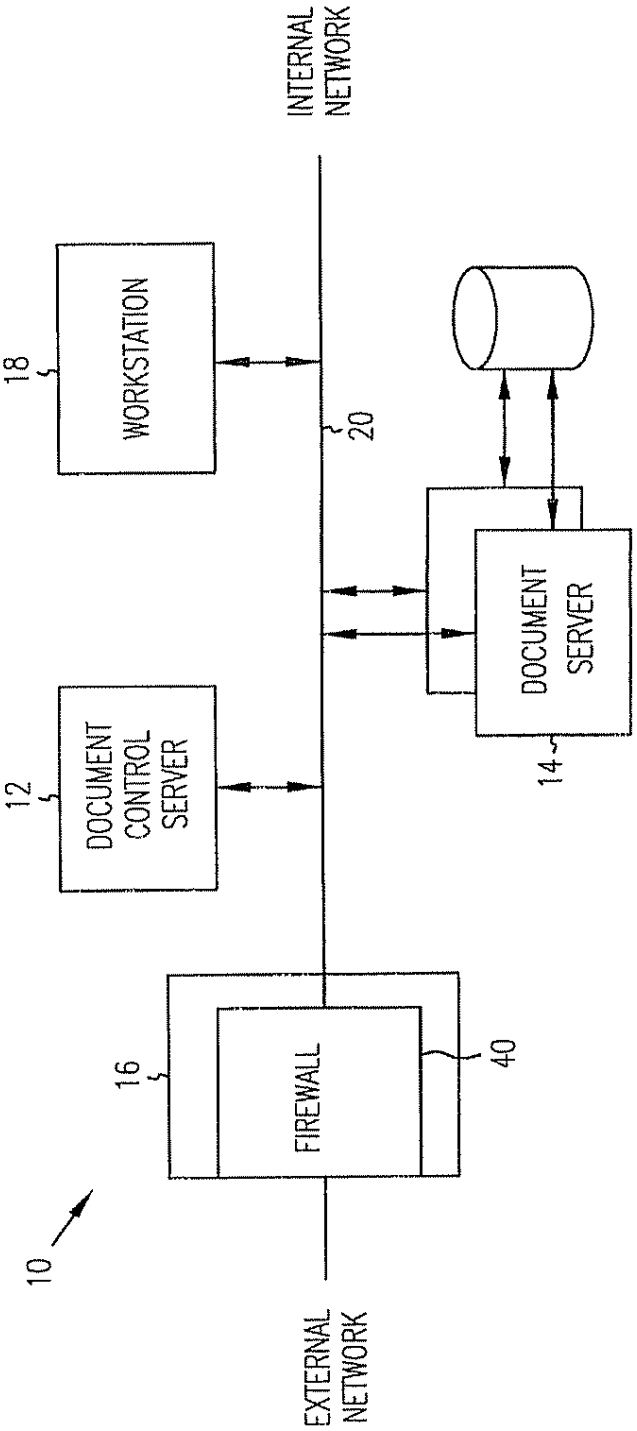

INTERNAL NETWORK
WORKSTATION
18
20
DOCUMENT SERVER
14
DOCUMENT CONTROL SERVER
12
FIREWALL
16
40
10
EXTERNAL NETWORK

FIG. 4

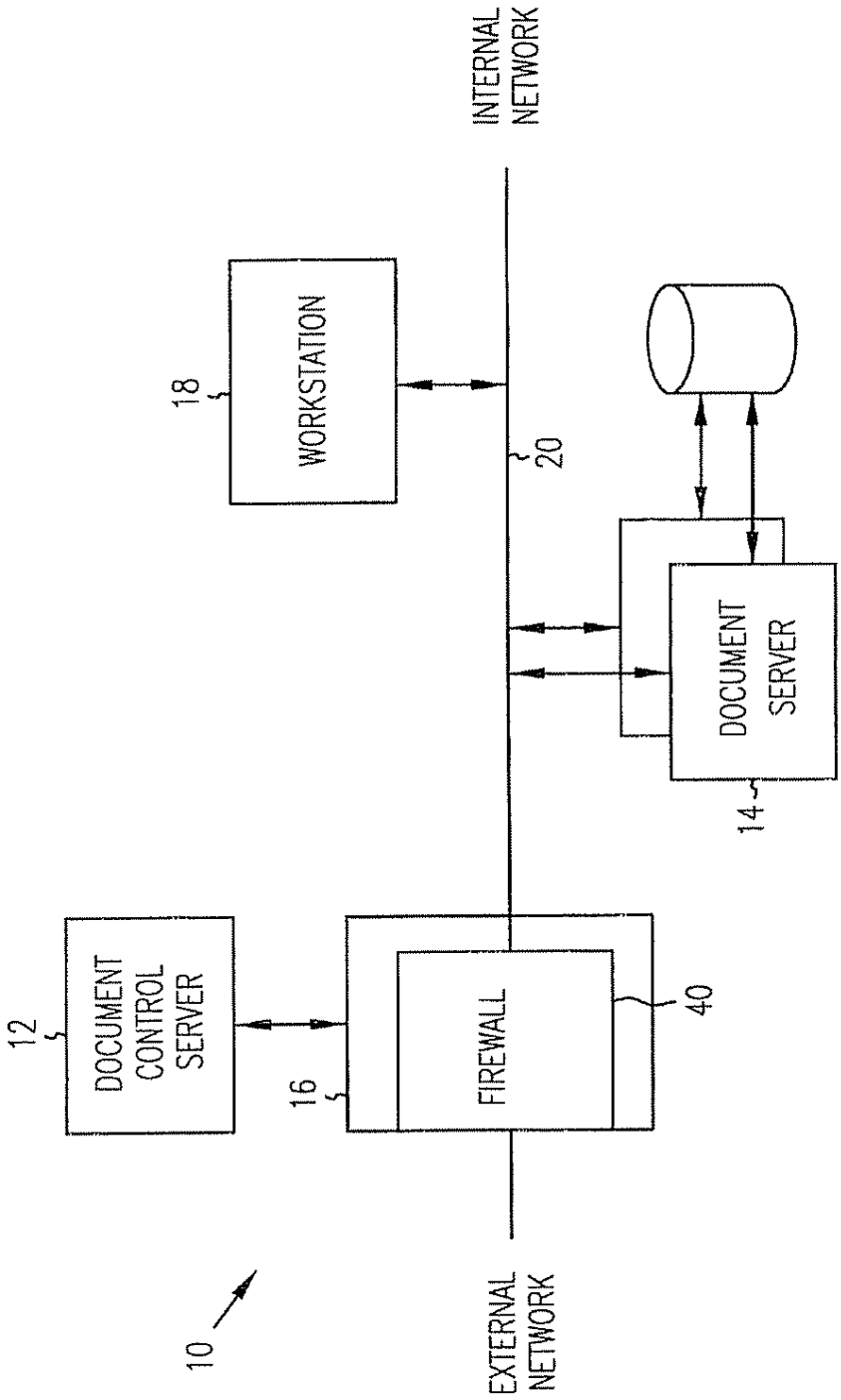

INTERNAL NETWORK
WORKSTATION
18
20
DOCUMENT SERVER
14
DOCUMENT CONTROL SERVER
12
16
FIREWALL
40
EXTERNAL NETWORK
10

FIG. 5

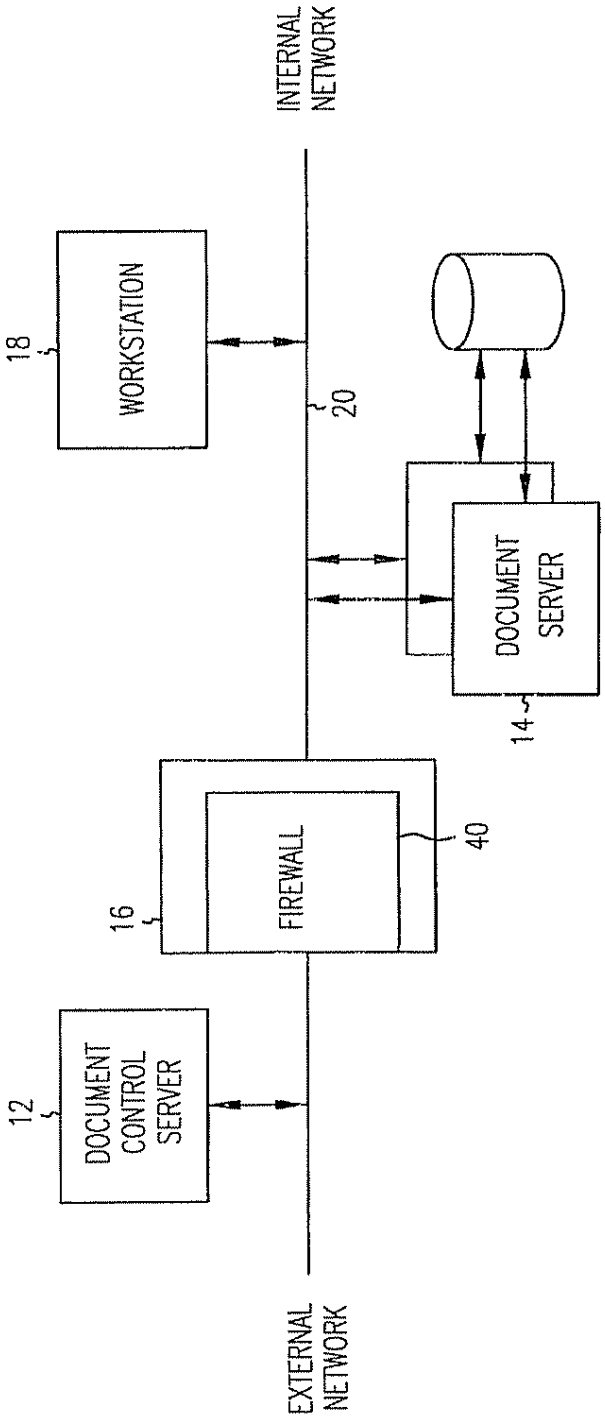

INTERNAL NETWORK
WORKSTATION
18
20
DOCUMENT SERVER
14
FIREWALL
40
16
DOCUMENT CONTROL SERVER
12
EXTERNAL NETWORK

FIG. 6

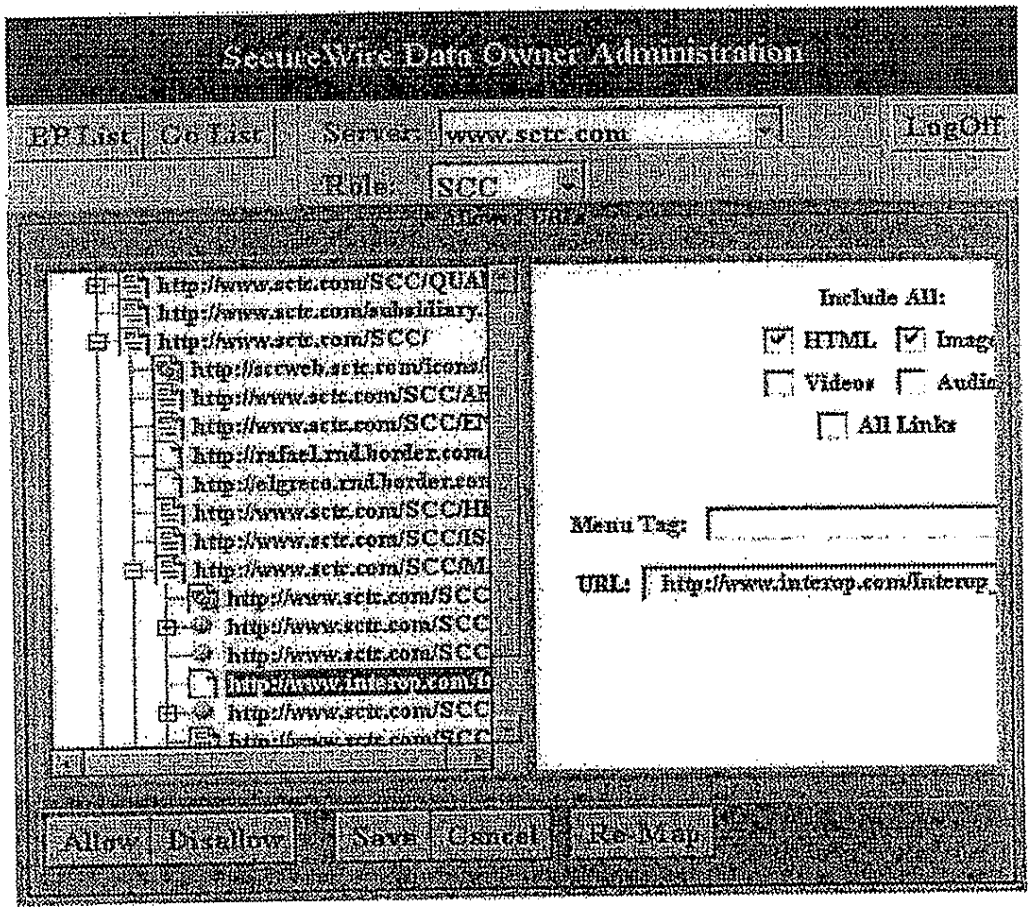

SecureWire Data Owner Administration
EP List
Cc List
Server:
www.sctc.com
LogOff
Role:
SCC
Include All:
HTML
Image
Video
Audio
All Links
Menu Tag:
URL:
http://www.interop.com/interop
Allow
Disallow
Save
Cancel
Re Map

FIG. 7

SYSTEM AND METHOD FOR CONTROLLING ACCESS TO DOCUMENTS STORED ON AN INTERNAL NETWORK

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and methods for controlling communication between networks, and in particular to a system and method for limiting access to documents stored on an internal network

2. Background Information

Businesses today are acting cooperatively to achieve compatible business goals For example, companies are using just-in-time manufacturing techniques to reduce overhead. To make this work, companies rely heavily on the ability of their suppliers to provide materials when needed.

At the same time, in this digital age business executives have become accustomed to receiving information from a number of sources both inside and outside the company almost instantaneously. They rely on such information to drive their day-to-day management decisions.

In order to provide outside organizations with relevant information in a timely manner, many companies have expanded their order-processing departments to handle increased call volumes. In this environment, outside partners call into the company's order-processing department to request specific information. This requires an employee to be available to answer calls, pull up information and verbally convey information to the partner. This option is very expensive, slow, and offers a poor level of service What is needed is a system and method of streamlining the flow of information between partner companies while limiting access to company proprietary information.

The Internet provides one possible solution to this problem. The nature of the Internet makes it an ideal vehicle for organizations to communicate and share information. The Internet offers low cost universal access to information Because of this, Internet transactions are expected to more than quadruple over the next two years, and partner communications via the Internet will almost double Companies have begun to look to the Internet as a medium allowing quick, easy and inexpensive to business partners To date, however, their Internet options have been limited.

One solution is to give business partners access to the company internal network Companies are hesitant to do this, however, since such access, if abused, can lead to the disclosure of company sensitive information

Another solution is to replicate necessary information to a web server located outside the company'firewall. Such an approach does allow organizations direct access to the information while at the same time limiting their access to company sensitive information. For this environment to work, however, the MIS department must manually transfer information from the internal network to the external server. Therefore, while this option offers organizations direct access to necessary data, that information can be 24 to 48 hours old When dealing with just-in-time inventory levels and large dollar amounts, 24 hours is too late. This option also creates a bottleneck in MIS, redundancy of data, and decreased data integrity

What is needed is a system and method for giving controlled access to designated documents stored on the internal network while restricting access to company sensitive information

SUMMARY OF THE INVENTION

The present invention is a system and method of limiting access from an external network to documents stored on an internal network A client list is built in which each client is assigned to one or more roles Each role has access to one or more documents as defined on a document list. A request from an external network is reviewed and, if possible, the request is associated with a client on the client list. The requested document is then compared to the document list associated with the client'role and, if the requested document is in the list of documents available to a client in the client's role, the requested document is fetched, cleaned and sent to the client.

According to another aspect of the present invention, a document control system is described. The document control system includes an internal network, an external interface, a document server connected to the internal network, and a document control server connected to the internal network and to the external interface. The document server controls access to a plurality of documents, including a first document. The document control server includes a go list processor for determining if the user has authorization to access said first document and a document processor for reading the first document from the document server, cleaning the first document and forwarding a clean version of said first document to the user. In operation, the document control server receives a document request from the external interface for the first document, determines a user associated with the document request, authenticates the user, determines if the user has authorization to access said first document and, if authorized, reads the first document from the document server, cleans the first document and forwards a clean version of said first document to the user

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings, where like numerals refer to like components throughout the several views,

FIG. 1 shows a document access system;

FIG. 2 is a flow diagram illustrating operations performed by the document access system of FIG 1;

FIG. 3 shows a document control server which can be used in the document access system shown in FIG. 1;

FIG 4 is a document access system which includes a firewall;

FIG. 5 is a document access system in which the document control server is placed in a third network;

FIG. 6 is a document access system in which the document control server is placed on the external network; and

FIG. 7 is an example of a tree structure representation which could be used to aid the data owner in the selection of permitted URLs.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

As noted above, corporations today are required by customers to deliver information such as price changes, new product data, manufacturing data, and customer support electronically. Competition is driving firms to work with partners through tight connections to internal systems Allowing access, however, to such data in an efficient, manageable, and secure manner presents challenges. Com-

panies go to great lengths to set up order processing departments and replicate large quantities of internal data to an external Internet server These efforts are not only inefficient, but usually result in redundancy of data, decreased network integrity, and a bottleneck in the MIS department

The present invention solves this problem by allowing specified external users controlled, customized, and secure access to the company's intranet without complex network infrastructure modifications Further, the present invention permits one to control the parts of a Web server that are accessible to a Business Partner with only minimal intervention by IS personnel (The term "Business Partner" is used in the following discussion to describe an external user who needs access to data such as Web pages which are not generally available to the public, but who also should not have unlimited to a company's intranet Web services)

A document access system for giving controlled access to designated documents stored on the internal network while restricting access to company sensitive information is shown in FIG 1 In FIG 1 document access system 10 includes a document control server 12, a document server 14, an external interface 16 and one or more internal workstations 18 Document control server 12, document server 14, external interface 16 and internal workstations 18 are interconnected via internal network 20 Document server 14 reads and writes documents to storage 20 Requests for documents arrive at external interface 16 and are forwarded to document control server 12 for execution In one embodiment external interface 16 includes a router used to form an Internet connection In another embodiment, external interface 16 includes a direct connection interface such as formed by one or more modems used for direct dial-up by business partners wishing to access their data

In one embodiment, as is illustrated in FIG 2, at 30 document control server 12 receives a document request from the external interface for a first document At 32, document control server 12 determines a user associated with the document request and authenticates the user At 34, system 10 checks to see if the user is authorized to access the document requested If so, at 36, system 10 retrieves the document from document server 14, cleans the document at 38 and, at 40, forwards the clean version of the document to the user One embodiment of such a system and method is described next for a HyperText Transfer Protocol (HTTP) system

When an HTTP or HTTPS connection request comes into document control server 12 there are three critical functions that must take place prior to returning the requested Web page: authentication, authorization, and internal connection If either of the first two functions fail, the internal connection is not made Then, once the internal connection has been made, document control server 12 must parse and "clean" the Web page prior to returning it to the requesting user

Authentication

Authentication is fairly straight-forward and is of course visible to the end user Following the HTTP protocol, when a user first enters a Uniform Resource Locator (URL) from their browser and the request is received at 30 (see FIG 2) at server 12, a check is made at 32 for authentication If basic authentication is being used, a check is made for authentication information in the HTTP header If no username and password are found, the server returns a 401 error to the browser, telling the browser it needs to authenticate The browser then pops up the box prompting the user to enter a username and password When the HTTP request comes into the server, document control server 12 parses the username and password, comparing against its internal database of users and if it finds a match, lets control proceed onto the authorization step If no match is found, document control server 12 returns an error code back to the Web server it is running under (e g , Internet Information Server or Netscape Enterprise Server) and the server will once again send back a 401 requesting the username and password This process can happen 3 times and then the server will deny access In one embodiment this authentication check is checked against a data base of known users as opposed to letting the Web Server check against a user database it may have

Authorization

Once document control server 12 has authenticated the request, it must, at 34, determine if the user is authorized to get to the URL they have requested This authorization will fail if the URL the user requested is not in the list of "allowed" URLs associated with the user In one embodiment, each user is assigned one or more roles Each role has access to a set of allowed URLs associated with that role

In one embodiment each user has one or more roles associated with their user ID For instance, they could be in the Marketing role, as well as the Engineering role In one such embodiment, each role is directly associated with an internal server; you can only define one role for each server This means you could not have the Marketing role and the Engineering role going to the same physical internal server Such an approach can simplify system design

In another embodiment, more than one roles may be assigned to each internal server For example, a manufacturer may have all his reseller information on one server One role, however, contains international resellers and another role contains domestic resellers In such an embodiment, it would be advantageous to be able to define different sets of URLs on a single document server 14 that would allow for the different roles

To complete the authorization portion, document control server 12 scans the list of allowed URLs for each role the user is in until it finds a match If no match is made, an error condition is returned to the Web server indicating access is denied and the Web server in turn sends the appropriate error back to the browser

An important and unique point to make here is that document control server 12 must translate the URL prior to doing its search for a match on the URL When an external business partner (user) enters the URL, they enter a URL where the first part of the URL points document control server 12 and the second portion is the 'role' associated with that URL

e g., https://www <server ID> com/Engineering/Standards/http_protocol html

where

https=Secure http connection using SSL,

www <server ID> com=DNS name of document control server 12 (this name is unique to the customer installation)

/Engineering=role associated with this particular URL

/Standards/http_protocol html=actual web page on the internal web server

If the real intranet web server associated with the Engineering role were engineer abcd com, then the translated URL that document control server 12 would search for is:

engineer.abcd com/Standards/http_protocol html

Note, the next two sections, Intranet connection and parsing the page, are entirely invisible to the end user

Intranet Connection

If both the authentication and authorization phases completed successfully, document control server 12 will open a

TCP connection to the appropriate intranet server (engineer.abcd.com from the above example) Once the TCP connection has been made, document control server 12 generates an http request for the specific web page The intranet server locates and returns the requested web page to document control server 12.

Parsing the Page

The pages returned by the intranet are categorized as either text or non-text. Examples of the latter are graphics, such as GIF or JPEG documents, sound objects, or executable objects, such as Java applets. Non-text pages are not parsed and forwarded back to the client browser unchanged Text documents, such as HTML formatted pages, however, contain embedded links that may need to be translated into their external equivalent. Embedded links fall into 3 groups, some of which require translation, while others don't: relative path links, server path links and absolute path links.

Relative path links, which are of the form subdir/page html, don't require translation because the browser will prepend the path based on the referrer's page For example, if the referrer's page was at:

http://www.document__control__server com/Engineering/Standards/http__protocol htm

and the relative link was ssl__protocol html, then the browser would prepend

http://www.document__control__server.com/Engineering/Standards/to the link.

Server path links take the form of /Specification/wheel.html and require translation This type of link points to a page that resides on the same server as the referrer's page, but with an absolute path starting at the root directory of the server. Assuming the same referrer's page as in the paragraph above, the translated link would be /Engineering/Specification/wheel.html (Note that the access string http:// is not required because the browser will fill that in) The translation is performed by prepending the alias associated with the referrer's page, Engineering, in this case, to the path of the embedded link.

Absolute path links are full URLs, such as

http://engineer.abcd.com/Performance/testdrive html

and require translation only if they point to a server that is in document control server 12's Alias table The example link will get translated because it points to the server engineer.abcd.com that exists in document control server 12's Alias table as Engineering. The translation is done by replacing the intranet server's name by the document control server 12's server name, followed by the alias of the intranet server. In this example, the translated URL would be

http://www.<server 12 ID>.com/Engineering/Performance/testdrive.html.

Links that point to pages on servers unknown to document control server 12 are not translated because they may well point to valid external sites, such as Yahoo, which should be left untouched In one embodiment, therefore, these links are not translated. (Note that if the referrer'page came in through the Secure Socket Layer (SSL), i.e., the URL starts with https://, then the translated links will also have https://)

On the other hand, such links could pose a security threat. That is, the link could be pointing to an intranet server that contains sensitive information, whose existence should not be revealed to external users. To counter this, in one embodiment document control server 12 includes a list of links which should be hidden from the outside world. Links found on such a list would be translated to something innocuous.

Redirection

When a page has moved, an intranet server may send a redirect status back to document control server 12. This means that document control server 12 has to translate the redirected address, similar to how embedded links are handled, before forwarding it to the client browser.

Architecture

A document access system such as system 10 illustrated in FIG. 1 enables users to grant outside organizations direct access to internal web data in a secure, simple and manageable way. It is essentially a secure window through which outside partners can view internal web data If, as is shown in FIG. 4, external interface 16 includes a firewall 40, system 10 also provides authenticated, authorized and view-customized business partner access to key Intranet servers via a standard web browser. Such a system enables users to easily, but accountably, grant authenticated partner access to internal web data, with complete control and authorization. Outside partners need only access a predefined URL in order to access an internal web page.

In one embodiment, as is shown in FIG. 4, document control server 12 is installed inside firewall 40. In another embodiment, as is shown in FIG. 5, document control server 12 is installed on a third network. Either way document control server 12 authenticates the outside user and then routes the request to a hidden, internal URL. The entire process is transparent to the outside user, and easily defined by the internal document control server 12 user. This allows business partners direct access to the data, eliminating the time lag, redundancy, lack of integrity and the bottleneck within the MIS Dept. (Please note that if document control server 12 is installed inside the firewall as is shown in FIG. 4, firewall 40 must be configured to restrict HTTP requests from any external source so that they can only get through to server 12. Similarly, if document control server 12 is installed on a third network (as a type of demilitarized zone (DMZ)) as is shown in FIG 5, firewall 40 must be configured to restrict HTTP requests into internal network 20 so that they can only come from server 12.)

In a third embodiment, such as is shown in FIG. 6, document control server 12 is installed outside firewall 40 and is accessed through the Secure Sockets Layer (SSL). Such an embodiment should be set up so that firewall 40 allows HTTP traffic only from document control server 12 into internal network 20.

To further reduce any bottleneck, in one embodiment document control server 12 includes the option for the actual "data owners" themselves to define which partners have access to selective internal data. A data owner is a trusted individual within the organization that is empowered to grant Business Partners access privileges to Web pages on document servers 16. In one such embodiment, a Data Owner is assigned to one or more "roles," where a "role" represents the mapping alias assigned to one or the servers 16. A Data Owner can only add Business Partners or map URLs for the server "role" to which the Data Owner is assigned.

For example, an employee working in the Accounting department would be assigned to an Accounting role (server) The Accounting Data Owner is only able to access the internal servers specified by the administrator. This prevents the Accounting Data Owner from mapping URLs on any other server such as the Marketing or Engineering servers.

Once a Data Owner has been assigned to a role, he or she is able to perform the following tasks:

Add, modify, or delete a Business Partner from that particular role

Establish a user ID and password for a Business Partner for basic authentication

Post or map an internal URL for access by a Business Partner

Delete URLs from a posted Go List

Delegation of such tasks to the data owners frees up MIS while also delegating data administration to those who understand the information best. In such an embodiment, the system administrator also defines general authentication rules and the list of eligible document servers **16**.

Business Partners are somewhat-trusted end users. They can be granted controlled access to selected Web page structures on internal Web servers(s) such as document servers **16** once they have been provided with the following information:

A URL connecting them to document control server **12**.

A user ID and password to authenticate them to document control server **12**.

The name of the "menu tag" that they will select when they connect to document control server **12** that will retrieve the internal Web pages as specified by the Data Owner.

It is the Data Owners' responsibility to create and maintain a listing of Business Partners that require access to the intranet servers they control and provide the Business Partner with the information they will need to access the selected intranet server(s)

Every Business Partner defined by a Data Owner is part of a "group." The "group" a Business Partner belongs to is directly related to the role a Data Owner has been assigned and what internal servers are associated with that role. These groups control what URLs they are able to access on the internal servers.

A Business Partner can be assigned to multiple groups. For example, a Business Partner may belong to both the Marketing and the Sales groups Data Owners manage their Business Partner accounts through the Business Partner list. From the Business Partner List, a Data Owner can establish a new Business Partner and modify or delete an existing Business Partner to any groups that they control.

In one embodiment, a Business Partner List is accessed by clicking on a BP List button on a Data Owner Administration utility window.

In one embodiment, document control server **12** includes a go list processor **22** and a document processor **24** (see FIG. **3**). Go list processor **22** determines if the user has authorization to access said first document. Document processor **24** reads a document from document server **14**, cleans the document as detailed above and forwards a clean version of the document to the user. Go list processor **22** and document processor **24** will be discussed next.

a) The Go List

The Go list is used by the document control server **12** to determine which URLs an authenticated Business Partner may be allowed to display. The Go List is unique to each role It is identified by the rolename data within the roles/directory. In one embodiment, the Go List is managed by MIS. Such an embodiment does not, however, take advantage of the flexibility provided by the architecture of the present invention Instead, it can be advantageous to permit individual data owners to determine the URLs to be included in each Go List Such an embodiment will be discussed next. In this example, documents are made available by the Data Owner and can be accessed by a user termed a "business partner (BP)".

In one such embodiment, the Go list contains data formatted as follows:

Real_url; MENU="menu_name"

where the Real URL is the actual URL (without the http://) used by document control server **12** to access that particular directory or file. The MENU parameter is always present. There can be a value within the quotes, or it can be empty. If there is a value within the quotes, then document control server **12** will parse that value up and set up a link to that particular URL with the title of the link being the Menu Name—if the Business Partner goes to its menu page after it logs in.

Only allowed URLs are present within the go list. No other URLs are included.

Also, the Go List will permit the Business Partner to access any of the files under a certain directory. For the time being, this is done by default on any URL that the user allows that ends with a"/"—to allow the Business Partner to access anything within the subdirectory—this is entered in the go list with the traditional '*' following the trailing slash. In one embodiment, the directory URL as kept intact and the Data Owner is given the option to cut and paste the path that the Data Owner wants the whole directory included in. In such an embodiment Data Owners append the * to the directory name if they want everything within that directory accessible to the Business Partners within that role. In another embodiment, explicit "disallows" could be included to handle documents the Data Owner wants to except from inclusion in the list of accessible documents.

b) The Mapping Code on Document Control Server **12**

The next portion of the whole mapping design is where a lot of the real work comes into play. There is some code within document control server **12** that gets called when the user (Data Owner) wants to map a particular server to the Go List. In one embodiment, a graphical user interface is used to select URLs and business partners. In one such embodiment, this code gets activated by the Data Owner performing one of the following tasks:

(A) Bringing up the Server Go List for the first time

(B) Clicking on a Node within the Go List Mapping Tree that has not yet been expanded and may have some children node

(C) Clicking on the Remap Button

At this point the GUI communicates to Server **12** via a Get URL request. The Get URL request:

(A) indicates to the server to load the GO list for a particular role

(B) checks to see if the node has not already been expanded and that the node exists on this server (the front part of the URL indicating the server name is consistent) and that the node is of an html type (or directory type)—if the node matches all of these criteria, then the GUI will indicate to the server to expand the particular URL for the particular role and

(C) If the DO selects the Remap button, they are prompted to see if they want to remap that portion of the server down. If the DO selects yes, then a request to Remap with the currently selected URL and the role is sent to the server.

Server **12** then acts upon the request that it receives from the GUI

(A) if the request was to load the GO list, then the server portion checks for the existence of a role_map data file in the roles directory. If this file does exist, then all that is done is that file is sent to the GUI line by line as is. If the file does not exist, then the file is created and the

mapping function is called. The mapping function is called with the file pointer, the name of the URL (the server name) to be mapped, and a depth indicator of 1. (NOTE: This embodiment includes an option to go down multiple layers, however due to timeout issues it may be better to just go down one layer at a time and let the user build the map as they see fit. If it goes down multiple layers than the mapping function must have the skills and capabilities to prevent the same URL from being mapped multiple times (the recursive nature of links and web spiders). The mapping code and its behavior is described below these ordered steps.)

Once the mapping code is done, then the URLs with their appropriate line syntax have been input and saved into the mapping file. The mapping file is then sent line by line to the GUI.

(B) If the request was to expand a node, the server code then calls the mapping function for the particular URL to be expanded. It opens up a temp file to be used to write the information into. It then calls the mapping code with a file pointer to this temp file, the URL to be mapped, and a depth of 1. (NOTE: same code called as in condition A, just different parameters). Once the mapping code returns, the file is communicated line by line to the GUI and then the file is removed from the system.

(C) If the request was to Remap a particular server or URL, then things get a little tricky. If the DO had chosen to remap the entire server, then the URL sent is the base URL—otherwise the URL sent was the URL that the DO wanted to remap from that point down. The same code is used regardless of the situation—just a different URL value. What happens is:

The current map file is copied over to the new map file until the line with the URL to be remapped is read in.

At this point this line is parsed to determine the depth in the tree (root level is 0).

A remap function is called which then does the following (note, that this is complicated by the fact that the tree could be at varying depths with files having been added or deleted and we would like to keep the prior shape and values of the tree when applicable).

Create a temp file to contain the intermediate results of the mapping.

Call the map function with a pointer to the temp file, the URL, and a depth of 1.

It then compares the current map file line by line with the temp file.

If the URL at the current depth is not found in the respective depth in the new temp file, that URL and any URLs immediately following it with a depth greater than the current depth are removed (that initial file is missing).

If the URL at the current depth is found in the temp file, any URL lines in between the URL being searched for and the prior URL are new files and are added prior to the current URL in the map file. Their syntax lines indicate the current depth and default of disallowing that URL. Then the existing current URL line is left as is in the map file.

At this point the next URL in the map file needs to be examined, in examining this URL the URL line syntax is examined. The depth is the issue of primary concern. If the depth is the same as the current depth, then continue with this loop. If the depth is a depth deeper than the current depth, then this URL is a child of the prior URL and the prior URL then also needs to be remapped—the remap function is then called recursively with the prior URL. If the depth is less than the current depth, then we are no longer examining URLs that needed to be remapped and this function then returns.

After the final remap function returns, the remainder of the values are not to be touched and so they are copied over to the new map file as is.

After the server is done remapping, it then sends the whole newly mapped tree back to the GUI line by line. (NOTE: the server also then recreates the Go list to reflect the new values, information on creating the Go list from the mapping information is below.)

Finally, the GUI reads in the lines of information it gets from the server.

For (A) an initially loaded server, the GUI will create a tree examining each line of input. This is described in section 3 of this summary.

For (B) an expanded node, the GUI will create children nodes immediately below the expanded nodes by setting the depth according to the new tree and parsing each line of input. The parsing of the lines of input is described in section 3 of this summary.

For (C) a remapped server, the GUI will delete the previous tree and re-create the new tree (similar to A).

The code that does the mapping is a set of code pieces that loads the URL, parses any HTML that is returned, and creates a chain of information regarding the links. It then searches however deep is desired on each of the links.

it uses some standard libraries to aid in parsing and getting the URL and HTML.

when it encounters a link, it stores that information in memory. At that time it also attempts to determine what sort of file it is—currently we only distinguish between the following: HTML, sound, graphic, external, video. It attempts to determine this based off of the hints surrounding it based on the filename and the surrounding html.

If the file is an HTML file and the mapping code has not yet reached the requested depth of mapping, the mapping code with then recursively try to bring up the HTML file and parse through its contents, etc.

As it comes across a file and finishes parsing it—it creates a syntax line that the GUI is expecting and writes this line to the file that it is passed. The line is as follows:

URL (just a tag) http://real_file _url (the is the URL to the file that the mapping code downloaded and parsed—this is the file that will be allowed or denied by the DO)

depth (an integer that is to indicate the current depth that this file is in the tree—the lines are listed such that the tree can be loaded via a depth—first sort of algorithm—it continues down the left hand side while the depth is getting bigger, adding children from left to right as the depth is the same, and going back up the tree as the depth becomes smaller)

filename (this is the name of the file for that URL—a * is used if the filename cannot be determined (like in the case of a directory or the server)

file type (this is a character which corresponds to the filetypes that were previously mentioned)

state of node (this is a character which indicates if this node was in a collapsed or expanded state when the tree

was saved—this is used by the GUI only, the mapping code always defaults this to C)

allowed (this is a character which indicates if this URL is to be allowed or disallowed, the mapping code defaults this to disallowed)

status of attaining the link (this is the HTTP status code of trying to access this link

it could have a value of 200 which means it was accessed OK, 404 meaning that this URL was not found, or a 0 indicating that this was not accessed)

already mapped (this is a one character flag used to indicate if this URL was already mapped and exists previously in the tree or not, this is most useful in a multi-depth mapping search)

Finally, the server has one more responsibility with respect to the mapping code. The server must handle writing out the saved data from the GUI when the DO requests to save the data. At this point, the data that is posted from the GUI to the server is written out line by line into the map file again. After this is done, the server deletes the prior Go List and parses through the map file a line at a time determining if that line is allowed. If the line is allowed the real_url part of the Map line is added (minus the http://) to the Go List. Next, the server checks the line to see if a "Menu" tag has been appended, if so, the server then adds the appropriate Menu tag to the Go list. Otherwise, it just adds a null menu tag to the Go list. As mentioned previously, currently if the real_url ends in a '/' an '*' is appended to the end of the real_url line to indicate that the user can access the entire directory—see Section 1 for further information.

After the Go List has been saved, the server is re-initialized with the new values—thus allowing immediate access or denial of access to the Business Partners for that role.

The Directory Map with the GUI

As mentioned previously, in one embodiment the GUI reads in and interprets the given line in order to creating nodes to represent the mapped server as a tree structure to the DO. Once such tree structure can be seen in FIG. 7.

The GUI communicates with server 12 as previously discussed and gets back well-defined lines of data. It parses the data and creates a node for each line provided by the Go list. It then looks at the expanded and collapsed feature to determine whether that node should be expanded or collapsed. It also looks at the file type to associate an image with that node. This image should allow the user to better determine what sort of nodes they are giving the Business Partners access to. The image is also determined by the return status from the mapping process—if a status of 404 is specified, then that link is determined to be broken (at least from document control server 12) and a broken link icon is displayed next to it. Finally, if that node is currently allowed, then the green ball is displayed next to it—to given the illusion of "green light means Go" to the DO.

The directory tree is created in a depth first fashion. It reads in each line examining the current depth. If the depth of the new node to be inserted is greater than the current depth than the node is inserted as a child of the previously inserted node. If the depth is the same, than it is inserted as a sibling. If the depth is less, then the tree is parsed back until the depth of the tree is at the same value of the depth and the node is inserted as a sibling at that level. The server is considered to be at the root level and thus has a depth of 0.

The text value that shows up with the node in the tree is the real_url value minus the http:// appended by the Menu Tag and Value if there is one for that node. A node may have a menu tag without being allowed.

The Data Owner (DO) can then traverse the tree examining the various links and determining what to allow and what to disallow. If they allow a directory—everything beneath that directory will be allowed. There currently is no mechanism for handling exceptions yet. If they allow files, then that file is allowed. If they have checked any other "include on allow" options (currently we offer, include all Gifs, Audio, Video, HTML, All Links)—then the files immediately beneath (once again only one layer deep) are automatically turned to allow if they are of the corresponding type. One note is that external files will never be "allowed"—as they do not exist on the server and thus it does not make sense for the DO to be allowing or disallowing those files.

When a data owner selects a link, they have the option of specifying the menu tag to be shown. If they do not specify one, then it is left blank. If they do then it is assigned for that node only. In order for it to get assigned to that node, the DO will have to select Allow or Disallow.

When Data Owners have finished making their changes they can save or cancel their mapping values. If they cancel then nothing that they did since their last save or remap will be saved. If they hit save, the values are communicated back to the server and the map file and the Go List File are updated as described previously.

Installation

Prior to install: Before fully installing and configuring document control server 12, the customer must have a digital certificate (for SSL encryption or transmissions) as well as set up and configure a server such as Internet Information Server (on NT) or Netscape Enterprise Server (on UNIX Solaris).

Installations: MIS installs document control server 12 onto the IIS or NES server and configures the firewall to allow HTTP access to the document control server 12 server.

Definition of end users: Document control server 12 offers organizations the option to delegate administration to end users who control the actual data (Data Owners) rather than forcing more work onto MIS. The data owner'access is defined by the network administrator. The data owner then maps which servers can be accessed. This data is stored in the document control server 12 "go list." The program code implementing document control server 12 is now completely installed, and ready for use.

Define business partner access: At this point, in order for an outside partner to access data, he/she must be granted access by the data owner. The data owner simply accesses the document control server 12 "data owner" GUI via a standard Java-enabled web browser. He/She can then define the new partner via role-based administration or explicitly choose which URLs may be accessed.

Outside users will not have access to any internal URL that is not specifically listed, even if there are embedded links in a URL for which access was granted. However, users can define access to a particular URL and all sub-pages as well.

Future partner access: After one role has been defined, future partners need only be added to that role, rather than requiring a whole new access to be defined.

Business partner access: All the outside partner has to do is type in the defined URL with any standard web browser. The partner will then be prompted for a user ID and password. Once these are entered, the partner will see a list of accessible URLs.

Back End Databases

It is important to understand that document control server 12 simply passes HTML information. This means document

control server 12 does not have a problem passing CGI scripts and other dynamic content. Where this becomes particularly confusing is the access and authentication to back end databases via an application gateway

One of document control server 12's greatest values is to allow outsiders access to ever-changing information such as order processing, shipping, etc. Much of this data is stored in large back-end databases with an application gateway on the front end. The application gateway puts an HTML front end on the database and allows Intranet users to query required information. Typically, a user only needs to enter a customer account number to access this information. However, in order to give outside users direct access, many organizations need to require some level of authentication to this process.

When document control server 12 passes an outside partner to any Intranet URL, the user is authenticated as a unique document control server 12 user, however, that user ID is not passed on to the Intranet server. Therefore, direct access to back end databases cannot be defined for each document control server 12 Business Partner. It will be necessary to create an HTML-based sign-in screen. This is a simple process and offers an opportunity for resellers and professional services to add value to the product sale.

Many Internet web servers handle restricted access in slightly different ways. If the user is not known, the web server responds with a 401 error. The user's browser then displays a standard screen requesting user ID and password. The user types these in and is granted access.

It is important to understand that document control server 12 cannot process this transaction. For security reasons, only HTTP traffic can pass through document control server 12. Any authentication must be HTTP based, as mentioned above.

In one embodiment, document control server 12 is installed on a standard web server running IIS (NT) or NES (Solaris). It requires no changes to the current infrastructure, and no "agents" or "clients" to be installed on any web servers or browsers.

Administration and data owner usage is accessed via document control server 12's Java user interface. This allows access via any web browser that supports Java (e.g., Internet Explorer 4.0, Netscape 4.0). Outside partner access is also accomplished via a standard web browser.

Operating with Third Party Firewalls

Document control server 12 can be used in conjunction with a firewall to add an additional layer of security to Business Partner communications via the Web. Two components need to be considered when determining the location of document control server 12: Domain Name Service (DNS) and routing.

Depending on the deployment option preferred and the capabilities of firewall 40, there are up to four different methods for routing traffic to, and through, server 12:

1) Redirected proxy—For added security on external to internal connections, a redirected proxy can be configured on your firewall to redirect the inbound connection requests. When a Business Partner on the external network attempts to connect to document control server 12, firewall 40 intercepts the request and establishes a connection to server 12. This rerouted connection hides the actual destination from the Business Partner requesting the connection.

2) Transparent proxy—A transparent proxy can be set up through firewall 40 to document control server 12. From the Business Partners' perspective it will appear as though they are connecting directly to server 12 and not connecting to the firewall first.

3) Directly to document control server 12—If document control server 12 is installed on the external side of firewall 40 (as in FIG. 6), connection requests will be routed directly to server 12. In such an embodiment, server 12 authenticates the Business Partner, and passes the request through firewall 40. Firewall 40 then retrieves the requested Web page(s) from the specified document server 16.

4) Through a third network—(some firewalls allow a "third network" capability, (sometimes called the DMZ or the Secure Server Network). The three deployment scenarios discussed above still apply in a "three network" environment, however, additional firewall configuration is necessary to ensure that the required name resolution (DNS), and routing are still possible.

Security Features SSL encryption. In one embodiment, data transmitted between the partner and web server is SSL-encrypted to prevent a sniffer from gathering information from the connection.

Document control server 12 server encrypted. Data stored on document control server 12 server such as user IDs, the go list, and partner profiles are all encrypted to prevent unauthorized access.

Password and user ID authentication. In one embodiment, document control server 12 supports password and user IDs for authorization. Stronger encryption could also be used.

Granular Access Controls

Business partners can only access internal URLs to which explicit access is given. If an accessible URL has embedded links to pages to which explicit access has not been granted, the partner cannot connect to them. However, if an embedded link is to an outside server, such as www.yahoo.com, in one embodiment access will not be restricted.

Internal URLs and IP Address Are Hidden

To ensure the security of the internal network and web pages, internal URLs and IP addresses are hidden from outside access. Partners type in a predefined URL and are presented with a list of accessible internal URLs. When a link is selected from the list Document control server 12 then maps to the internal URL. The internal URL and IP address are never displayed for the partner to see.

System Requirements, Compatibility and Performance

Considerations for performance and reliability include amount of cache memory, CPU power, BUS speed, amount of RAM, speed of memory chips, bus architecture (IDE, EIDE, PCI etc.), hard drive capacity, and hard drive quality (seek and access speeds). The following table identifies the basic characteristics of minimum, recommended and ideal server configurations to run document control server 12.

System Component	Minimum	Recommended	Ideal
CPU	Pentium 166	Pentium 200	Pentium Pro 200
RAM	32 MB	48 MB	64 MB
Hard disk	1 GB	2 GB	4 GB
Platform	IIS 3.0 (NT 4.0) or NES 3.0 (Solaris 2.5.1)		
Browser	Java enabled web browser MS Internet Explorer 4.0 or higher Netscape Navigator 4.0 or higher with Netscape's JDK 1.1 patch		
Other	CD-ROM, 3.5" diskette, Color monitor, Keyboard, Mouse		

Document control server 12 enables users to easily, but accountably, grant authenticated partner access to internal web data, with complete control and authorization. Outside partners need only access a predefined URL in order to access an internal web page.

The following examples provide a better idea of how document control server 12 can be used to meet a variety of needs.

Example—Manufacturing (Order Processing)

Manufacturing companies process thousands of orders every day. In order to keep up with competition and to achieve the highest levels of quality, customers/partners need to know the immediate status of an order to the minute. Many companies today have moved to just-in-time inventory systems to reduce overhead and costs. Document control server 12 can grant access directly to an order-processing page that connects directly into an order-processing database. The order-processing agents (data owners) can define what data customers/partners have direct access to. As a result, the customer knows immediately the status of an order. The supplier also saves money by eliminating the need to replicate data or take phone calls asking for updates.

Example—Distribution

A distribution environment operates an order-processing and shipping department very similar to manufacturing. However, distribution also requires various types of information to be distributed to different partners, such as pricing and quantity breaks. Document control server 12 allows a company to customize the view each distributor or reseller sees, such as pricing or quantity breaks.

Example—Financial Services

Financial institutions process millions of transactions a day with a large number of outside partners. These include the purchase and sale of assets as well as order/sale confirmation, etc. Today, many of these transactions require a third party to set up a secure certificate. Document control server 12 can speed up this entire process by allowing an agent to immediately allow an outside customer or partner access to trading information in minutes, and without the need for third-party intervention.

Example—Health Services

Health care and insurance organizations process thousands of claims each day. Partners need a secure way to pass medical information and process it into a company's systems. For example, a doctor treats a patient who has Blue Cross/Blue Shield. That doctor needs to know if the patient's insurance covers the treatment, then process the claim after the treatment is given, and finally check on the status of payment once a claim is submitted. With document control server 12, Blue Cross/Blue Shield can give the doctor's office access to their internal list of insured patients, as well as the status of current claims. The company no longer needs to replicate this data to a DMZ or SSN Internet server or handle a phone call. The doctor's office can also securely fill out a web-based claim form over the Internet to process the claim for treatment.

Example—Government Agency

It is necessary for various government agencies and departments to frequently share sensitive data. One example is the CIA and various law enforcement agencies. The FBI, DEA, ATF and other agencies must routinely check into the files of various personnel and public citizens. Typically, this requires these agencies to send a paper request for information to the CIA. The CIA must then search for the relevant information and then send a copy back to the requesting agency.

With document control server 12, the FBI and other agencies can be given direct access to the CIA files that might be relevant such as histories and fingerprint analysis databases. This can save time and money.

Document control server 12 offers several advantages over current methods such as cost savings, improved customer service and leveraging of the current infrastructure. Current methods for passing data to outside partners are expensive, slow and unreliable. Document control server 12 offers the information to partners faster, easier and cheaper. It also more tightly integrates partners, thus improving business relations. Document control server 12 also leverages the benefits of current technology such as the Internet and Intranet.

Other business advantages of document control server 12 include: it reduces overhead and costs; it eliminates the need to copy content to a web server within the DMZ or external network; it offers spontaneous, dynamic user-managed content; it eliminates the wait for an IS manager to update data or post on a web server; it eliminates integrity and replication issues; it more tightly integrates partners; and its open architecture allows access without the need to alter current technology.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiment shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is intended that this invention be limited only by the claims and the equivalents thereof.

What is claimed is:

1. A method of limiting access from an external network to documents stored on an internal network, the method comprising:

building a client list, wherein building a client list includes assigning each client to a role;

building a document list naming documents available to clients assigned to the client's role;

receiving a request for a document stored on the internal network;

associating the request with a client;

determining if the requested document is on the list of documents; and

if the requested document is on the list of documents, fetching the requested document as a proxy and sending the requested document to the client.

2. The method according to claim 1, wherein each document has a unique URL and wherein the document list includes the URL of each available document, wherein the step of determining includes the step of determining if the URL of the requested document is included in the document list.

3. The method according to claim 2, wherein building the document list includes displaying available documents in a tree structure within a graphical user interface, wherein displaying includes querying a document control server to obtain a current version of the document list.

4. The method according to claim 1, wherein associating the request with a client includes the step of authenticating the client.

5. The method according to claim 4, wherein each document has a unique URL and wherein the document list includes the URL of each available document, wherein the step of determining includes the step of determining if the URL of the requested document is included in the document list.

6. The method according to claim 5, wherein building the document list includes displaying available documents in a tree structure within a graphical user interface, wherein

displaying includes the step of querying a document control server to obtain a current version of the document list.

7. A document control system, including:

an internal network;

an external interface;

a document server connected to the internal network, wherein the document server controls access to a plurality of documents, including a first document; and

a document control server, wherein the document control server receives a document request for the first document, determines a user associated with the document request and authenticates the user, wherein the document control server includes a go list processor for determining if the user has authorization to access said first document and a document processor for reading the first document from the document server, cleaning the first document and forwarding a clean version of said first document to the user

8. The document control system according to claim 7, wherein the external interface includes a firewall connected to an external network, wherein the document control server communicates to the document server through the firewall.

9. The document control system according to claim 7, wherein the document processor acts as a proxy to hide access to the first document.

10. The document control system according to claim 7, wherein the external interface includes a telephone interface into which a business partner can dial to gain access to the document control server.

11. A document control system, including:

an internal network;

an external interface;

a document server connected to the internal network, wherein the document server controls access to a plurality of documents, including a first document;

a document control server; and

a data owner interface for building a document list of available documents;

wherein the document control server receives a document request from the external interface for the first document, determines a user associated with the document request and authenticates the user; and

wherein the document control server includes a go list processor for determining, based on the document list, if the user has authorization to access said first document.

12. The document control system according to claim 11, wherein the data owner interface includes a graphical user interface which displays the document list in a tree structure, wherein the graphical user interface queries the document control server to obtain a current version of the document list

13. The document control system according to claim 11, wherein the document control server further includes a document processor for reading the first document from the document server, cleaning the first document and forwarding a clean version of said first document to the user

14. The document control system according to claim 13, wherein the document processor acts as a proxy to hide access to the first document

15. The document control system according to claim 14, wherein the data owner interface includes a graphical user interface which displays the document list in a tree structure, wherein the graphical user interface queries the document control server to obtain a current version of the document list.

16. The document control system according to claim 11, wherein the external interface includes a firewall connected to an external network

17. The document control system according to claim 11, wherein the external interface includes a telephone interface into which a business partner can dial to gain access to the document control server.

18. The document control system according to claim 8, wherein the document control server is connected to the external network and communicates to the firewall through the external network.

19. The document control system according to claim 8, wherein the document control server is connected to a third network and communicates to the firewall through the third network.

20. The document control system according to claim 7, wherein the document control server is connected to the internal network and wherein the external interface includes a firewall connected to an external network, wherein the firewall is configured to receive the document request and to route the document request to the document control server.

21. The document control system according to claim 7, wherein the document control server includes means for translating links embedded in the first document

22. The document control system according to claim 7, wherein each user is assigned one or more roles and wherein the go list processor restricts access to documents as function of the role under which the user attempts to access the document.

23. In a system having an internal network and an interface to an external network, a method of handling requests from the external network for documents stored on the internal network, the method comprising:

defining one or more users;

defining documents accessible to the users;

receiving a document request from the external network;

determining a user associated with the document request;

authenticating the user associated with the document request;

determining if the user associated with the document request has permission to access the document requested; and

if the user associated with the document request has permission to access the document requested, retrieving the document requested from the internal network, cleaning the document of embedded links and delivering the document to the user associated with the document request.

24. The method according to claim 23, wherein each document has a unique URL and wherein determining if the user associated with the document request has permission to access the document requested includes:

accessing a document list listing the URL of each available document; and

generating an error message if the document requested is not on the document list.

25. The method according to claim 23, wherein defining documents accessible to the users includes assigning each

user to one or more roles and limiting access to documents as a function of role and wherein determining if the user associated with the document request has permission to access the document requested includes determining if users in the role associated with the document request have permission to access the document requested.

26. The method according to claim 24, wherein defining documents accessible to the users includes assigning each user to one or more roles and limiting access to documents as a function of role and wherein determining if the user associated with the document request has permission to access the document requested includes determining if users in the role associated with the document request have permission to access the document requested.

27. The method according to claim 23, wherein each document request includes an HTTP header and wherein authenticating the user associated with the document request includes retrieving authentication information from the HTTP header.

28. The method according to claim 23, wherein cleaning the document of embedded links includes looking for a server path link and replacing the server path link with a link to an alias.

29. The method according to claim 23, wherein cleaning the document of embedded links includes looking for an absolute path link, determining if the absolute path link is a link which should be hidden and, if the absolute path link is a link which should be hidden, replacing the absolute path link with a different link.

30. In a system having an internal network and an interface to an external network, a method of handling requests from the external network for documents stored on the internal network, the method comprising:

defining a plurality of users, including a first and a second user;

assigning each user to one or more roles, wherein assigning includes assigning the first user to a first role and the second user to a second role;

defining documents accessible to the users, wherein defining includes limiting access to documents as a function of the roles assigned to the user;

receiving a document request from the external network;

determining a user and a role associated with the document request;

authenticating the user associated with the document request;

determining if users in the role associated with the document request have permission to access the document requested; and

if users in the role associated with the document request have permission to access the document requested, retrieving the document requested from the internal network and delivering the document to the user associated with the document request.

31. The method according to claim 30, wherein each document has a unique URL and wherein determining if the user associated with the document request has permission to access the document requested includes:

accessing a document list listing the URL of each available document; and

generating an error message if the document requested is not on the document list.

32. The method according to claim 30, wherein retrieving the document requested includes cleaning the document of embedded links.

33. The method according to claim 32, wherein cleaning the document of embedded links includes looking for a server path link and replacing the server path link with a link to an alias.

34. The method according to claim 32, wherein cleaning the document of embedded links includes looking for an absolute path link, determining if the absolute path link is a link which should be hidden and, if the absolute path link is a link which should be hidden, replacing the absolute path link with a different link.

35. A computer-readable medium having program code for limiting access from an external network to documents stored on an internal network, the program code comprising:

program code for building a client list, wherein program code for building a client list includes program code for assigning each client to a role;

program code for building a document list naming documents available to clients assigned to the client'role;

program code for receiving a request for a document stored on the internal network;

program code for associating the request with a client;

program code for determining if the requested document is on the list of documents; and

program code for, if the requested document is on the list of documents, fetching the requested document as a proxy and sending the requested document to the client.

36. A computer-readable medium comprising program code, in a system having an internal network and an interface to an external network, for handling requests from the external network for documents stored on the internal network, the program code comprising:

program code for defining one or more users;

program code for defining documents accessible to the users;

program code for receiving a document request from the external network;

program code for determining a user associated with the document request;

program code for authenticating the user associated with the document request;

program code for determining if the user associated with the document request has permission to access the document requested; and

program code for, if the user associated with the document request has permission to access the document requested, retrieving the document requested from the internal network, cleaning the document of embedded links and delivering the document to the user associated with the document request.

37. A computer-readable medium comprising program code, in a system having an internal network and an interface to an external network, for handling requests from the external network for documents stored on the internal network, the program code comprising:

program code for defining a plurality of users, including a first and a second user;

program code for assigning each user to one or more roles, wherein assigning includes assigning the first user to a first role and the second user to a second role;

program code for defining documents accessible to the users, wherein defining includes limiting access to documents as a function of the roles assigned to the user;

program code for receiving a document request from the external network;

program code for determining a user and a role associated with the document request;

program code for authenticating the user associated with the document request;

program code for determining if users in the role associated with the document request have permission to access the document requested; and

program code for, if users in the role associated with the document request have permission to access the document requested, retrieving the document requested from the internal network and delivering the document to the user associated with the document request.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,357,010 B1
DATED : March 12, 2002
INVENTOR(S) : Viets et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page,
Item [54], delete "**SYSTEM AND METHOD FOR CONTROLLING ACCESS TO DOCUMENTS STORED ON AN INTERNAL NETWORK**" and insert -- **ACCESS CONTROL TO INTERNAL NETWORK DOCUMENTS WITH CLIENT LIST ASSIGNING CLIENT'S ROLE AND DOCUMENT LIST NAMING DOCUMENTS AVAILABLE TO CLIENTS ASSIGNED TO CLIENT'S ROLE** --, therefor.

Column 1,
Line 48, delete "company'firewall" and insert -- company's firewall --, therefor.

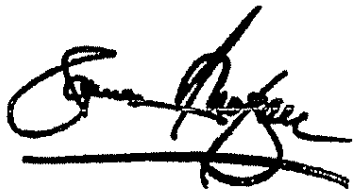
Column 2,
Line 7, delete "client'role" and insert -- client's role --, therefor.

Column 4,
Line 28, delete "roles" and insert -- role --, therefor.

Column 20,
Line 23, delete "client'role" and insert -- client's role --, therefor.

Signed and Sealed this

Twenty-fifth Day of March, 2003



JAMES E ROGAN
Director of the United States Patent and Trademark Office

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

RULE 7.1 DISCLOSURE STATEMENT FOR FINJAN SOFTWARE LTD

Defendant, Finjan Software Ltd. ("Finjan Israel") is a corporation organized and existing under the laws of Israel. Finjan Israel is a wholly owned subsidiary of Finjan Software, Inc. ("Finjan USA").

Dated: June 29, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli
Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
Telephone: 612.332.5300
Facsimile: 612.332.9081
Email: tzeuli@merchantgould.com
Email: mailto:jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: mailto:lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

Defendant, Finjan Software, Inc. ("Finjan USA") is a corporation organized and existing under the laws of the state of Delaware.

The following publicly held corporations own ten percent (10%) or more of Finjan USA's stock:

Cisco Systems, Inc. (NASDAQ: CSCO)

Dated: June 29, 2007

FINJAN SOFTWARE LTD., AND
FINJAN SOFTWARE, INC.,

s/Anthony R. Zeuli
Anthony R. Zeuli, MN Bar No. 0274884
J.R. Maddox, MN Bar No. 329253
Merchant & Gould P.C.
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
Telephone: 612.332.5300

Facsimile: 612.332.9081
Email: tzeuli@merchantgould.com
Email: mailto:jmaddox@merchantgould.com

Of Counsel:

Paul Andre
Lisa Kobialka
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025
Telephone: 650.838.4300
Facsimile: 650.838.4350
Email: pandre@perkinscoie.com
Email: mailto:lkobialka@perkinscoie.com

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp., Plaintiff, v. Finjan Software Ltd., and Finjan Software, Inc. Defendants.	)	Case No: 0:07-cv-02198-JMR-FLN

CERTIFICATE OF SERVICE

I hereby certify that on June 29, 2007, I caused the following documents:

1. **MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE;**
2. **CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 7.1;**
3. **DECLARATION OF EZRA SOFER IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE;**
4. **DECLARATION OF ANTHONY R. ZEULI IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE WITH ACCOMPANYING EXHIBITS A-D**
5. **RULE 7.1 DISCLOSURE STATEMENT FOR FINJAN SOFTWARE LTD.,**
6. **RULE 7.1 DISCLOSURE STATEMENT FOR FINJAN SOFTWARE, INC. and**
7. **CERTIFICATE OF SERVICE**

to be filed electronically with the Clerk of Court through ECF, and that ECF will send an e-notice of the electronic filing to the following counsel of record:

- **Trevor J Foster -** tjfoster@rkmc.com; dgterry@rkmc.com
- **Jacob M Holdreith -** jmholdreith@rkmc.com; dgterry@rkmc.com
- **Ronald J Schutz -** rjschutz@rkmc.com; lvlind@rkmc.com; crketterling@rkmc.com
- **Christopher A Seidl -** caseidl@rkmc.com; cjjunker@rkmc.com

I further certify that I caused the proposed order to be filed with the court via e-mail to the following judge who is hearing the motion:

- Chief Judge James R. Rosenbaum

And I certify that I caused a copy of the proposed order to be e-mailed as noted below to the following counsel of record:

- **Trevor J Foster -** tjfoster@rkmc.com; dgterry@rkmc.com
- **Jacob M Holdreith -** jmholdreith@rkmc.com; dgterry@rkmc.com
- **Ronald J Schutz -** rjschutz@rkmc.com; lvlind@rkmc.com; crketterling@rkmc.com
- **Christopher A Seidl -** caseidl@rkmc.com; cjjunker@rkmc.com

Dated: June 29, 2007

s/Anthony R. Zeuli
Anthony R. Zeuli

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)	Civil Action No. 07-CV-2198 JMR/FLN

STIPULATED PROTECTIVE ORDER

WHEREAS, discovery in the above entitled litigation may involve the disclosure of confidential trade secret, technical know-how, or other confidential or proprietary research, development, commercial, personal, financial information or information furnished in confidence by a third party (hereinafter individually and collectively referred to as "confidential material") relating to the subject matter of this litigation, regardless of how generated;

WHEREAS, the parties desire to limit the extent of disclosure and use of such confidential material, and to protect such confidential material from unauthorized use and/or further disclosure, and wish to insure that no advantage is gained by any party by the use of such confidential material which could not have been learned had discovery in this litigation has not occurred.

NOW, THEREFORE, IT IS STIPULATED AND AGREED by and between the parties, through their respective counsel, subject to the approval of the Court, that a

Protective Order pursuant to Rule 26(c) of the Federal Rules of Civil Procedure be entered as follows.

IT IS ORDERED THAT:

1. This Protective Order shall apply to all information, documents, electronic documents, things, discovery responses and testimony designated in good faith as constituting or containing confidential material by parties and non-parties in this litigation. Any confidential material produced by a party or non-party in this litigation may be designated by such party or non-party as (1) "CONFIDENTIAL" or (2) "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under the terms of this Protective Order.

2. For the purposes of this Protective Order, confidential material designated as "CONFIDENTIAL" shall be information or tangible things that the producing party believes in good faith qualifies for protection under standards developed under Rule 26(c) of the Federal Rules of Civil Procedure, including trade secrets or other confidential research, development, commercial or business information. Absent a specific order by this Court, once designated as “CONFIDENTIAL” such designated confidential material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such information shall not be disclosed to anyone except as provided herein.

3. Confidential material designated as “HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY” shall be information that the producing party believes in good faith is extremely sensitive confidential information whose disclosure to another

party or non-party would create a substantial adverse impact on the producing party's business, financial condition, ability to compete, standing in the industry or any other risk of injury that could not be avoided by less restrictive means. Such material includes, without limitation, information related to confidential technical or product information not released to the public; future projections, strategies, forecasts, or business plans; company financial information or financial analyses and projections that have not been made public; contractual relationships with third parties; identification of customers and vendors, materials relating to ongoing research and development efforts and future products; technical materials used solely for internal purposes in connection with development, production, engineering, or sales training; source code; and documents relating to the prosecution of patents that have not been issued and contain claims that are not publicly known. Absent a specific order by this Court, once designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," such designated material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such material shall not be disclosed to anyone except as provided herein.

4. Each party or nonparty that designates confidential material for protection under this Protective Order must take care to limit any such designation to specific material that qualifies under the appropriate standards. Mass, indiscriminate and routinized designations are prohibited. The designation of confidential material as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY"

for purposes of this Protective Order shall be made in the following manner by the party or non-party seeking protection:

(a) in the case of documents, electronic documents, exhibits, briefs, memoranda, interrogatory responses, responses to requests for admission, things or other materials (apart from depositions, pretrial or trial testimony): by affixing the legend "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, to every page of any document containing confidential material at the time such documents are produced or such information is disclosed, or as soon thereafter as the party or non-party seeking protection becomes aware of the confidential nature of the material disclosed and sought to be protected; and

(b) in the case of depositions, pretrial and trial testimony: (i) by a statement by counsel on the record during such deposition, pretrial or trial proceeding that the entire transcript or a portion thereof shall be designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, hereunder; or (ii) by written notice of such designation sent by counsel to all parties within twenty (20) calendar days of its receipt of the transcript of the testimony. The parties shall treat all deposition, pretrial and trial testimony as "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" hereunder until the expiration of twenty (20) calendar days of the receipt of the transcript. Unless so designated, any confidentiality is waived after the expiration of the 20-day period unless otherwise stipulated or ordered. The parties may modify this procedure for any particular

deposition or proceeding through agreement on the record at such deposition or proceeding or otherwise by written stipulation, without further order of the Court.

If confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" is used during the course of a deposition, that portion of the deposition record reflecting such confidential material shall be sealed and stamped with the designated degree of confidentiality, and access thereto shall be limited pursuant to the other terms of this Protective Order.

5. Confidential material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) Outside counsel for the parties identified as follows:

(1) For Plaintiff Secure Computing Corporation: Robins, Kaplan, Miller & Ciresi LLP.

(2) For Defendants Finjan Software, Ltd. and Finjan Software, Inc.: Perkins Coie LLP and Merchant & Gould P.C.

(3) As used herein, "outside counsel" shall mean attorneys for the respective firms, including supporting personnel employed by the attorneys, such as patent agents, paralegals, legal secretaries, legal clerks, and litigation support employees who are not presently involved in patent prosecution related to the subject matter of this litigation and will not be involved in *ex*

parte patent prosecution related to the subject matter of this litigation for three years following disclosure of the confidential material – this shall not preclude the recipient of confidential material from participating in *inter partes* or contested proceedings in a patent office.

(b) officers, directors and employees of the parties whose assistance is needed by counsel for the purposes of this litigation;

(c) no more than three individuals who serve as in-house counsel of each party where the assistance of that individual is needed by that party's counsel for the purposes of this litigation provided that for each individual provided access to material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof pursuant to this subsection, the party:

(1) provide the identity of the individual to all other parties in writing; and

(2) have the identified confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. A receiving party's outside counsel shall retain any such executed confidentiality agreements, and they need not be disclosed to the producing party unless the producing party, for good cause, requests a copy of such agreement(s).

(d) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(e) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(f) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(g) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(h) non-technical jury or trial consulting services retained by counsel for a party;

(i) the author(s) and all recipients of the document or the original source of the information; and

(j) any other person only upon order of the Court or upon written consent of the party producing the confidential material, subject to and conditioned upon compliance with Paragraph 8 herein.

6. Confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) parties' outside counsel of record in this litigation, as defined in paragraph 5(a) above;

(b) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(c) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(d) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(e) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(f) non-technical jury or trial consulting services retained by counsel for a party;

(g) any other person only upon order of the Court or upon written consent of the party producing the confidential information or material subject to and conditioned upon compliance with Paragraph 8 herein.

7. For purposes of Paragraphs 5(c) and 6(b) herein, a consultant or expert shall be defined as a person who is neither an employee, agent or representative of a party, nor anticipated to become an employee, agent or representative of a party in the near future, and who is retained or employed to assist in the preparation for trial in this litigation, whether full or part time, by or at the direction of counsel for a party. The procedure for having a consultant or expert approved for access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" shall be as follows:

(a) Outside counsel for the receiving party shall (i) provide the individual with a copy of this Protective Order, (2) explain its terms, and (3) obtain the

individual's written agreement, in the form of Exhibit A hereto, to comply with and be bound by its terms. Within five (5) court days of signing Exhibit A, the receiving party must identify in writing the individual to the producing party and provide the producing party with an executed Exhibit A and a written statement setting forth that person's present residence address, business address, employer, job title, any past or present association with any party, any litigation that the individual has provided any professional services during the preceding five years, and a current curriculum vitae;

(b) The receiving party that sends the identification specified in the preceding paragraph may disclose confidential material to the identified individual unless, within five (5) court days of delivering the identification, the party receives a written objection, served by facsimile or electronic mail, to the identification, setting forth in detail the grounds on which it is based. If a party receives such an objection, the individual shall be barred from access to the confidential material for a fourteen (14) calendar day period commencing with the receipt by the producing party of a copy of the executed Exhibit A;

(c) If within that fourteen (14) calendar day period, the parties are unable to resolve their differences and the opposing party moves for a further protective order, then the confidential material shall not be provided to said individual except by further order of the Court. Any such motion must describe the circumstances with specificity, set forth in detail the reasons for which the disclosure is reasonably necessary, assess the risk of harm that the disclosure would entail, and suggest any additional means that might be used to reduce that risk. The party opposing the disclosure to said

individual shall bear the burden of proving that the risk of harm that the disclosure would entail (under the safeguards proposed) outweighs the seeking party's need to disclose the confidential material to said individual.

8. All persons listed in Paragraphs 5(b), 5(f), and 5(g), above, and interpreters or translators referenced in Paragraph 5(e), may be given access to confidential material designated as "CONFIDENTIAL," provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. Similarly, all persons listed in Paragraphs 6(e) and 6(f) above, and interpreters or translators referenced in Paragraph 6(e), may be given access to confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A.

9. Any person may be examined as a witness at trial or during a deposition concerning any confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" which that person had lawfully received or authored prior to and apart from this litigation. During examination, any such witness may be shown confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by a party that appears on its face, or from other documents or testimony, to have been received from or authored by that witness or communicated to that witness. .

10. Confidential material may be filed with or presented to the Court, or may be included in briefs, memoranda or other papers filed with this Court, but if so, they shall be filed under seal in accordance with the Local Rules of the Court and the United States District Court for the District of Minnesota.

11. A party may challenge any other party's designation of confidential materials produced herein as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by serving a written objection upon the producing party. A party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed. In the event that a party challenges in writing, at any time during this litigation, the designation of confidential material, the designating party, shall, within fourteen (14) calendar days of such challenge, substantiate the basis for such designation in writing. If no substantiation is proffered, the material shall not be deemed designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order. If substantiation is offered, the parties shall first try to resolve such dispute in good faith on an informal basis. If the dispute cannot be resolved, the party challenging the claim of confidentiality may seek appropriate relief from the Court. Each such motion shall identify the challenged material and the basis for the challenge. Until a dispute over the asserted designation is finally resolved by the parties or the Court, all parties and persons shall treat the confidential material in question as designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY."

12. All counsel for the parties who have access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order acknowledge they are bound by this Order and submit to the jurisdiction of this Court for purposes of enforcing this Order.

13. Entering into, agreeing to, and/or producing or receiving confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or otherwise complying with the terms of this Protective Order shall not:

(a) waive any right to object on any ground to use in evidence of any of the confidential material covered by this Protective Order;

(b) waive any objection otherwise available to the disclosure or production of confidential material on any ground not addressed in this Protective Order.

14. This Protective Order has no effect upon, and shall not apply to, a party's use or disclosure of its own confidential material for any purpose. Nothing contained herein shall impose any restrictions on the use or disclosure by a party of confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" obtained lawfully by such party independently of any proceedings in this action, or which:

(a) was already known to such party by lawful means prior to acquisition from, or disclosure by, any other party in this action;

(b) is or becomes publicly known through no fault or act of such party; or

(c) is rightfully received by such party from a third party that has authority to provide such information or material and without restriction as to disclosure.

15. If a party inadvertently produces "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" material without marking it as such, it may be disclosed to others until the receiving party becomes aware of the error, unless it appears from the face of the document that it contains non-public, confidential, proprietary, commercially sensitive, or trade secret information of the producing party. As soon as the receiving party becomes aware of the inadvertent production, the information must be treated as if it had been timely designated under this Protective Order, and the receiving party must endeavor in good faith to obtain all copies of the material that it distributed or disclosed to persons not authorized to access such information by Paragraphs 5 and 6 above, as well as any copies made by such persons. If timely corrected, an inadvertent failure to designate confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" does not, standing alone, waive the producing party's right to secure protection under this Protective Order for such material.

16. If a party learns that, by inadvertence or otherwise, it has disclosed confidential material to any person or in any circumstance not authorized under this Protective Order, that party must immediately (1) notify in writing the designating party of the unauthorized disclosures, (2) use its best efforts to retrieve all copies of the confidential material, (3) inform the person or persons to whom unauthorized disclosures

were made of all the terms of this Order, and (4) request such person or persons complete and sign a copy of the undertaking in the form attached hereto as Exhibit A.

17. The production of confidential material which are alleged to have been inadvertently produced and are subject to the attorney client privilege, work product immunity or other protection from disclosure, shall not constitute a waiver of such privilege. After receiving notice from the producing party that confidential material subject to protection has been inadvertently produced, the receiving party shall not review, copy or disseminate such confidential material. The receiving party shall return such confidential material to the producing party immediately. Return of the confidential material by the receiving party shall not constitute an admission or concession, or permit any inference, that the returned material is, in fact, properly subject to a claim of attorney-client privilege, work product immunity, or other protection from disclosure, nor shall it foreclose any party from moving the Court for an order that such material has been improperly designated or should be discoverable and/or usable in this litigation for reasons other than a waiver caused by the inadvertent production.

18. It is the present intention of the parties that the provisions of this Protective Order shall govern discovery and other pretrial and trial proceedings in this action. Nonetheless, each of the parties hereto shall be entitled to seek modification of this Protective Order by application to the Court on notice to the other parties hereto for good cause.

19. The provisions of this Protective Order shall, absent written permission of the producing party or further order of the Court, continue to be binding throughout and

after the conclusion of this action, including without limitation any appeals therefrom. Within sixty (60) calendar days after receiving notice of the entry of an order, judgment, or decree finally disposing of this action, including any appeals therefrom, all persons having received confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" hereunder shall return such material and all copies thereof (including summaries and excerpts) to counsel for the producing party, or shall certify destruction thereof. Counsel described in paragraphs 5(a) and 6(a) above shall be entitled to retain court papers, deposition and trial transcripts, and attorney work product (including court papers, transcripts, and attorney work product that contain information or material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY") and to one copy of documents produced by the opposing party designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that such counsel, and employees of such counsel, shall not disclose any such information and material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" contained in such court papers, transcripts, attorney work product, or documents to any person or entity except pursuant to a written agreement with the producing party of the information or material. All materials returned to the parties or their counsel by the Court likewise shall be disposed of in accordance with this paragraph.

20. If any party (a) is subpoenaed in another action, (b) is served with a demand in another action to which it is a party, or (c) is served with any other legal

process by one not a party to this litigation, seeking information or material which was produced or designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by someone other than that party, the party shall give prompt actual written notice no more than five (5) court days of receipt of such subpoena, demand, or legal process, to those who produced or designated the confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" and shall object to its production to the extent permitted by law. Should the person seeking access to the confidential material take action against the party or anyone else covered by this Protective Order to enforce such a subpoena, demand or other legal process, the party shall respond by setting forth the existence of this Protective Order. The designating party shall bear the burdens and the expenses of seeking protection in that court of its confidential material, and nothing in these provisions should be construed as authorizing or encouraging a party in this action to disobey a lawful directive from another court.

21. The parties agree that all designated documents, information, and material exchanged between the parties and subject to this Protective Order in this action shall be used solely for the prosecution or defense of the claims in this action and shall not be used for any business, commercial, competitive, personal, or other purposes, subject to the other terms of this Protective Order.

22. Nothing in this Protective Order shall prevent outside or inside counsel from giving legal advice based on information that has been designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY"

provided such legal advice shall not reveal the substance of any designated information to a person who is not authorized to receive it.

23. The parties agree to be bound by the terms of this Protective Order pending its entry by the Court, or pending the entry of an alternative thereto which is satisfactory to all parties, and any violation of its terms shall be subject to the same sanctions and penalties as if the Protective Order had been entered by the Court.

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: _____/s/ Christopher A. Seidl_____
Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (#313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Attorneys for Plaintiff
Secure Computing Corp.

MERCHANT & GOULD P.C.

By: ___/s/ Anthony R. Zeuli_____
Anthony R. Zeuli (#274884)
J.R. Maddox, (#329523)
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
(612) 332-5300

Of Counsel:

Paul J. Andre
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114
(650) 838-4300

Attorneys for Defendants
Finjan Software, Ltd., and Finjan Software, Inc.

SO ORDERED, this ____ day of _____, 2007

_____
United States District Judge

Exhibit A
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)))))))))	Civil Action No. 07-CV-2198 JMR/FLN

STIPULATED PROTECTIVE ORDER

UNDERTAKING OF: _____

1. My home address is:

2. My present employer is and the address of my present employment is:

3. My present occupation or job description is:

4. I have received a copy of the Stipulated Protective Order in this litigation.

5. I have carefully read and understand the provisions of the Stipulated Protective Order in this litigation.

6. I will comply with all of the provisions of the Stipulated Protective Order.

7. I will hold in confidence, will not disclose to anyone not qualified under the Stipulated Protective Order, and will use only for purposes of this litigation, in strict compliance with the terms and conditions of the Stipulated Protective Order, any confidential material which is disclosed to me. I acknowledge that termination of the litigation does not release me from the obligations set out in this paragraph.

8. I will return all confidential information which comes into my possession, and documents or things which I have prepared relating thereto, to counsel for the party

by whom I am employed or retained in strict accordance with the provisions of the Stipulated Protective Order.

9. I hereby submit to the jurisdiction of this Court for the purposes of enforcement of the Stipulated Protective Order in this litigation.

10. Any accompanying resume or curriculum vitae is a complete and accurate statement to the best of my knowledge, and I acknowledge that in submitting such resume or curriculum vitae I know that the receiving party shall rely thereon.

11. I make the above statements under penalty of perjury.

Signature:_____
Date:_____

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.

Defendants.

Case No. 0:07-cv-2198 JMR/FLN

CERTIFICATE OF SERVICE

I hereby certify that on the 23rd day of July, 2007, I caused the following document:

STIPULATED PROTECTIVE ORDER

to be filed electronically with the Clerk of Court through ECF, and that ECF will send an e-notice of the electronic filing to the following counsel of record:

Anthony R. Zeuli tzeuli@merchant-gould.com

I further certify that a courtesy copy was delivered to Magistrate Judge Franklin L. Noel's chambers, and that the Stipulated Protective Order was filed with the court via e-mail to the following judge:

Magistrate Judge Franklin L. Noel noel_chambers@mnd.uscourts.gov

I certify that a copy of the Stipulated Protective Order was served on counsel via e-mail as follows:

Anthony R. Zeuli tzeuli@merchant-gould.com
James Hannah jhannah@perkinscoie.com

Dated: July 23, 2007

By: s/Christopher A. Seidl

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)	Civil Action No. 07-CV-2198 JMR/FLN

AMENDED STIPULATED PROTECTIVE ORDER

WHEREAS, discovery in the above entitled litigation may involve the disclosure of confidential trade secret, technical know-how, or other confidential or proprietary research, development, commercial, personal, financial information or information furnished in confidence by a third party (hereinafter individually and collectively referred to as "confidential material") relating to the subject matter of this litigation, regardless of how generated;

WHEREAS, the parties desire to limit the extent of disclosure and use of such confidential material, and to protect such confidential material from unauthorized use and/or further disclosure, and wish to insure that no advantage is gained by any party by the use of such confidential material which could not have been learned had discovery in this litigation has not occurred.

NOW, THEREFORE, IT IS STIPULATED AND AGREED by and between the parties, through their respective counsel, subject to the approval of the Court, that a

Protective Order pursuant to Rule 26(c) of the Federal Rules of Civil Procedure be entered as follows.

IT IS ORDERED THAT:

1. This Protective Order shall apply to all information, documents, electronic documents, things, discovery responses and testimony designated in good faith as constituting or containing confidential material by parties and non-parties in this litigation. Any confidential material produced by a party or non-party in this litigation may be designated by such party or non-party as (1) "CONFIDENTIAL" or (2) "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under the terms of this Protective Order.

2. For the purposes of this Protective Order, confidential material designated as "CONFIDENTIAL" shall be information or tangible things that the producing party believes in good faith qualifies for protection under standards developed under Rule 26(c) of the Federal Rules of Civil Procedure, including trade secrets or other confidential research, development, commercial or business information. Absent a specific order by this Court, once designated as “CONFIDENTIAL” such designated confidential material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such information shall not be disclosed to anyone except as provided herein.

3. Confidential material designated as “HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY” shall be information that the producing party believes in good faith is extremely sensitive confidential information whose disclosure to another

party or non-party would create a substantial adverse impact on the producing party's business, financial condition, ability to compete, standing in the industry or any other risk of injury that could not be avoided by less restrictive means. Such material includes, without limitation, information related to confidential technical or product information not released to the public; future projections, strategies, forecasts, or business plans; company financial information or financial analyses and projections that have not been made public; contractual relationships with third parties; identification of customers and vendors, materials relating to ongoing research and development efforts and future products; technical materials used solely for internal purposes in connection with development, production, engineering, or sales training; source code; and documents relating to the prosecution of patents that have not been issued and contain claims that are not publicly known. Absent a specific order by this Court, once designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," such designated material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such material shall not be disclosed to anyone except as provided herein.

4. Each party or nonparty that designates confidential material for protection under this Protective Order must take care to limit any such designation to specific material that qualifies under the appropriate standards. Mass, indiscriminate and routinized designations are prohibited. The designation of confidential material as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY"

for purposes of this Protective Order shall be made in the following manner by the party or non-party seeking protection:

(a) in the case of documents, electronic documents, exhibits, briefs, memoranda, interrogatory responses, responses to requests for admission, things or other materials (apart from depositions, pretrial or trial testimony): by affixing the legend "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, to every page of any document containing confidential material at the time such documents are produced or such information is disclosed, or as soon thereafter as the party or non-party seeking protection becomes aware of the confidential nature of the material disclosed and sought to be protected; and

(b) in the case of depositions, pretrial and trial testimony: (i) by a statement by counsel on the record during such deposition, pretrial or trial proceeding that the entire transcript or a portion thereof shall be designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, hereunder; or (ii) by written notice of such designation sent by counsel to all parties within twenty (20) calendar days of its receipt of the transcript of the testimony. The parties shall treat all deposition, pretrial and trial testimony as "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" hereunder until the expiration of twenty (20) calendar days of the receipt of the transcript. Unless so designated, any confidentiality is waived after the expiration of the 20-day period unless otherwise stipulated or ordered. The parties may modify this procedure for any particular

deposition or proceeding through agreement on the record at such deposition or proceeding or otherwise by written stipulation, without further order of the Court.

If confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" is used during the course of a deposition, that portion of the deposition record reflecting such confidential material shall be sealed and stamped with the designated degree of confidentiality, and access thereto shall be limited pursuant to the other terms of this Protective Order.

5. Confidential material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) Outside counsel for the parties identified as follows:

(1) For Plaintiff Secure Computing Corporation: Robins, Kaplan, Miller & Ciresi LLP.

(2) For Defendants Finjan Software, Ltd. and Finjan Software, Inc.: Perkins Coie LLP and Merchant & Gould P.C.

(3) As used herein, "outside counsel" shall mean attorneys for the respective firms, including supporting personnel employed by the attorneys, such as patent agents, paralegals, legal secretaries, legal clerks, and litigation support employees who are not presently involved in patent prosecution related to the subject matter of this litigation and will not be involved in *ex*

parte patent prosecution related to the subject matter of this litigation for three years following disclosure of the confidential material – this shall not preclude the recipient of confidential material from participating in *inter partes* or contested proceedings in a patent office.

(b) officers, directors and employees of the parties whose assistance is needed by counsel for the purposes of this litigation;

(c) no more than three individuals who serve as in-house counsel of each party where the assistance of that individual is needed by that party's counsel for the purposes of this litigation provided that for each individual provided access to material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof pursuant to this subsection, the party:

(1) provide the identity of the individual to all other parties in writing; and

(2) have the identified confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. A receiving party's outside counsel shall retain any such executed confidentiality agreements, and they need not be disclosed to the producing party unless the producing party, for good cause, requests a copy of such agreement(s).

(d) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(e) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(f) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(g) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(h) non-technical jury or trial consulting services retained by counsel for a party;

(i) the author(s) and all recipients of the document or the original source of the information; and

(j) any other person only upon order of the Court or upon written consent of the party producing the confidential material, subject to and conditioned upon compliance with Paragraph 8 herein.

6. Confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) parties' outside counsel of record in this litigation, as defined in paragraph 5(a) above;

(b) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(c) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(d) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(e) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(f) non-technical jury or trial consulting services retained by counsel for a party;

(g) any other person only upon order of the Court or upon written consent of the party producing the confidential information or material subject to and conditioned upon compliance with Paragraph 8 herein.

7. For purposes of Paragraphs 5(c) and 6(b) herein, a consultant or expert shall be defined as a person who is neither an employee, agent or representative of a party, nor anticipated to become an employee, agent or representative of a party in the near future, and who is retained or employed to assist in the preparation for trial in this litigation, whether full or part time, by or at the direction of counsel for a party. The procedure for having a consultant or expert approved for access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" shall be as follows:

(a) Outside counsel for the receiving party shall (i) provide the individual with a copy of this Protective Order, (2) explain its terms, and (3) obtain the

individual's written agreement, in the form of Exhibit A hereto, to comply with and be bound by its terms. Within five (5) court days of signing Exhibit A, the receiving party must identify in writing the individual to the producing party and provide the producing party with an executed Exhibit A and a written statement setting forth that person's present residence address, business address, employer, job title, any past or present association with any party, any litigation that the individual has provided any professional services during the preceding five years, and a current curriculum vitae;

(b) The receiving party that sends the identification specified in the preceding paragraph may disclose confidential material to the identified individual unless, within five (5) court days of delivering the identification, the party receives a written objection, served by facsimile or electronic mail, to the identification, setting forth in detail the grounds on which it is based. If a party receives such an objection, the individual shall be barred from access to the confidential material for a fourteen (14) calendar day period commencing with the receipt by the producing party of a copy of the executed Exhibit A;

(c) If within that fourteen (14) calendar day period, the parties are unable to resolve their differences and the opposing party moves for a further protective order, then the confidential material shall not be provided to said individual except by further order of the Court. Any such motion must describe the circumstances with specificity, set forth in detail the reasons for which the disclosure is reasonably necessary, assess the risk of harm that the disclosure would entail, and suggest any additional means that might be used to reduce that risk. The party opposing the disclosure to said

individual shall bear the burden of proving that the risk of harm that the disclosure would entail (under the safeguards proposed) outweighs the seeking party's need to disclose the confidential material to said individual.

8. All persons listed in Paragraphs 5(b), 5(f), and 5(g), above, and interpreters or translators referenced in Paragraph 5(e), may be given access to confidential material designated as "CONFIDENTIAL," provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. Similarly, all persons listed in Paragraphs 6(e) and 6(f) above, and interpreters or translators referenced in Paragraph 6(e), may be given access to confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A.

9. Any person may be examined as a witness at trial or during a deposition concerning any confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" which that person had lawfully received or authored prior to and apart from this litigation. During examination, any such witness may be shown confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by a party that appears on its face, or from other documents or testimony, to have been received from or authored by that witness or communicated to that witness. .

10. Confidential material may be filed with or presented to the Court, or may be included in briefs, memoranda or other papers filed with this Court, but if so, they shall be filed under seal in accordance with the Local Rules of the Court and the United States District Court for the District of Minnesota.

11. A party may challenge any other party's designation of confidential materials produced herein as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by serving a written objection upon the producing party. A party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed. In the event that a party challenges in writing, at any time during this litigation, the designation of confidential material, the designating party, shall, within fourteen (14) calendar days of such challenge, substantiate the basis for such designation in writing. If no substantiation is proffered, the material shall not be deemed designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order. If substantiation is offered, the parties shall first try to resolve such dispute in good faith on an informal basis. If the dispute cannot be resolved, the party challenging the claim of confidentiality may seek appropriate relief from the Court. Each such motion shall identify the challenged material and the basis for the challenge. Until a dispute over the asserted designation is finally resolved by the parties or the Court, all parties and persons shall treat the confidential material in question as designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY."

12. All counsel for the parties who have access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order acknowledge they are bound by this Order and submit to the jurisdiction of this Court for purposes of enforcing this Order.

13. Entering into, agreeing to, and/or producing or receiving confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or otherwise complying with the terms of this Protective Order shall not:

(a) waive any right to object on any ground to use in evidence of any of the confidential material covered by this Protective Order;

(b) waive any objection otherwise available to the disclosure or production of confidential material on any ground not addressed in this Protective Order.

14. This Protective Order has no effect upon, and shall not apply to, a party's use or disclosure of its own confidential material for any purpose. Nothing contained herein shall impose any restrictions on the use or disclosure by a party of confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" obtained lawfully by such party independently of any proceedings in this action, or which:

(a) was already known to such party by lawful means prior to acquisition from, or disclosure by, any other party in this action;

(b) is or becomes publicly known through no fault or act of such party; or

(c) is rightfully received by such party from a third party that has authority to provide such information or material and without restriction as to disclosure.

15. If a party inadvertently produces "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" material without marking it as such, it may be disclosed to others until the receiving party becomes aware of the error, unless it appears from the face of the document that it contains non-public, confidential, proprietary, commercially sensitive, or trade secret information of the producing party. As soon as the receiving party becomes aware of the inadvertent production, the information must be treated as if it had been timely designated under this Protective Order, and the receiving party must endeavor in good faith to obtain all copies of the material that it distributed or disclosed to persons not authorized to access such information by Paragraphs 5 and 6 above, as well as any copies made by such persons. If timely corrected, an inadvertent failure to designate confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" does not, standing alone, waive the producing party's right to secure protection under this Protective Order for such material.

16. If a party learns that, by inadvertence or otherwise, it has disclosed confidential material to any person or in any circumstance not authorized under this Protective Order, that party must immediately (1) notify in writing the designating party of the unauthorized disclosures, (2) use its best efforts to retrieve all copies of the confidential material, (3) inform the person or persons to whom unauthorized disclosures

were made of all the terms of this Order, and (4) request such person or persons complete and sign a copy of the undertaking in the form attached hereto as Exhibit A.

17. The production of confidential material which are alleged to have been inadvertently produced and are subject to the attorney client privilege, work product immunity or other protection from disclosure, shall not constitute a waiver of such privilege. After receiving notice from the producing party that confidential material subject to protection has been inadvertently produced, the receiving party shall not review, copy or disseminate such confidential material. The receiving party shall return such confidential material to the producing party immediately. Return of the confidential material by the receiving party shall not constitute an admission or concession, or permit any inference, that the returned material is, in fact, properly subject to a claim of attorney-client privilege, work product immunity, or other protection from disclosure, nor shall it foreclose any party from moving the Court for an order that such material has been improperly designated or should be discoverable and/or usable in this litigation for reasons other than a waiver caused by the inadvertent production.

18. It is the present intention of the parties that the provisions of this Protective Order shall govern discovery and other pretrial and trial proceedings in this action. Nonetheless, each of the parties hereto shall be entitled to seek modification of this Protective Order by application to the Court on notice to the other parties hereto for good cause.

19. The provisions of this Protective Order shall, absent written permission of the producing party or further order of the Court, continue to be binding throughout and

after the conclusion of this action, including without limitation any appeals therefrom. Within sixty (60) calendar days after receiving notice of the entry of an order, judgment, or decree finally disposing of this action, including any appeals therefrom, all persons having received confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" hereunder shall return such material and all copies thereof (including summaries and excerpts) to counsel for the producing party, or shall certify destruction thereof. Counsel described in paragraphs 5(a) and 6(a) above shall be entitled to retain court papers, deposition and trial transcripts, and attorney work product (including court papers, transcripts, and attorney work product that contain information or material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY") and to one copy of documents produced by the opposing party designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that such counsel, and employees of such counsel, shall not disclose any such information and material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" contained in such court papers, transcripts, attorney work product, or documents to any person or entity except pursuant to a written agreement with the producing party of the information or material. Within 60 days following the expiration of the last period for appeal from any order issued in connection with this action, the parties shall remove any materials designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" from the office of the Clerk of Court. Following that 60-day period, the Clerk of Court shall destroy all designated

"CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" materials.

20. If any party (a) is subpoenaed in another action, (b) is served with a demand in another action to which it is a party, or (c) is served with any other legal process by one not a party to this litigation, seeking information or material which was produced or designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by someone other than that party, the party shall give prompt actual written notice no more than five (5) court days of receipt of such subpoena, demand, or legal process, to those who produced or designated the confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" and shall object to its production to the extent permitted by law. Should the person seeking access to the confidential material take action against the party or anyone else covered by this Protective Order to enforce such a subpoena, demand or other legal process, the party shall respond by setting forth the existence of this Protective Order. The designating party shall bear the burdens and the expenses of seeking protection in that court of its confidential material, and nothing in these provisions should be construed as authorizing or encouraging a party in this action to disobey a lawful directive from another court.

21. The parties agree that all designated documents, information, and material exchanged between the parties and subject to this Protective Order in this action shall be used solely for the prosecution or defense of the claims in this action and shall not be

used for any business, commercial, competitive, personal, or other purposes, subject to the other terms of this Protective Order.

22. Nothing in this Protective Order shall prevent outside or inside counsel from giving legal advice based on information that has been designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided such legal advice shall not reveal the substance of any designated information to a person who is not authorized to receive it.

23. The parties agree to be bound by the terms of this Protective Order pending its entry by the Court, or pending the entry of an alternative thereto which is satisfactory to all parties, and any violation of its terms shall be subject to the same sanctions and penalties as if the Protective Order had been entered by the Court.

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: _____/s/ Christopher A. Seidl_____
Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (#313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Attorneys for Plaintiff
Secure Computing Corp.

MERCHANT & GOULD P.C.

By: ___/s/ Anthony R. Zeuli_____
Anthony R. Zeuli (#274884)
J.R. Maddox, (#329523)
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
(612) 332-5300

Of Counsel:

Paul J. Andre
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114
(650) 838-4300

Attorneys for Defendants
Finjan Software, Ltd., and Finjan Software, Inc.

SO ORDERED, this ____ day of _____, 2007

_____
United States District Judge

Exhibit A
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)))))))))	Civil Action No. 07-CV-2198 JMR/FLN

STIPULATED PROTECTIVE ORDER

UNDERTAKING OF: _____

1. My home address is:

2. My present employer is and the address of my present employment is:

3. My present occupation or job description is:

4. I have received a copy of the Stipulated Protective Order in this litigation.

5. I have carefully read and understand the provisions of the Stipulated Protective Order in this litigation.

6. I will comply with all of the provisions of the Stipulated Protective Order.

7. I will hold in confidence, will not disclose to anyone not qualified under the Stipulated Protective Order, and will use only for purposes of this litigation, in strict compliance with the terms and conditions of the Stipulated Protective Order, any confidential material which is disclosed to me. I acknowledge that termination of the litigation does not release me from the obligations set out in this paragraph.

8. I will return all confidential information which comes into my possession, and documents or things which I have prepared relating thereto, to counsel for the party

by whom I am employed or retained in strict accordance with the provisions of the Stipulated Protective Order.

9. I hereby submit to the jurisdiction of this Court for the purposes of enforcement of the Stipulated Protective Order in this litigation.

10. Any accompanying resume or curriculum vitae is a complete and accurate statement to the best of my knowledge, and I acknowledge that in submitting such resume or curriculum vitae I know that the receiving party shall rely thereon.

11. I make the above statements under penalty of perjury.

Signature:_____
Date:_____

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.

Defendants.

Case No. 0:07-cv-2198 JMR/FLN

CERTIFICATE OF SERVICE

I hereby certify that on the 24th day of July, 2007, I caused the following document:

AMENDED STIPULATED PROTECTIVE ORDER

to be filed electronically with the Clerk of Court through ECF, and that ECF will send an e-notice of the electronic filing to the following counsel of record:

Anthony R. Zeuli tzeuli@merchant-gould.com

I further certify that a courtesy copy was delivered to Magistrate Judge Franklin L. Noel's chambers, and that the Amended Stipulated Protective Order was filed with the court via e-mail to the following judge:

Chief Judge James M. Rosenbaum rosenbaum_chambers@mnd.uscourts.gov

I certify that a copy of the Amended Stipulated Protective Order was served on counsel via e-mail as follows:

Anthony R. Zeuli tzeuli@merchant-gould.com
James Hannah jhannah@perkinscoie.com

Dated: July 24, 2007 By: s/Christopher A. Seidl

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)	Civil Action No. 07-CV-2198 JMR/FLN

AMENDED STIPULATED PROTECTIVE ORDER

WHEREAS, discovery in the above entitled litigation may involve the disclosure of confidential trade secret, technical know-how, or other confidential or proprietary research, development, commercial, personal, financial information or information furnished in confidence by a third party (hereinafter individually and collectively referred to as "confidential material") relating to the subject matter of this litigation, regardless of how generated;

WHEREAS, the parties desire to limit the extent of disclosure and use of such confidential material, and to protect such confidential material from unauthorized use and/or further disclosure, and wish to insure that no advantage is gained by any party by the use of such confidential material which could not have been learned had discovery in this litigation has not occurred.

NOW, THEREFORE, IT IS STIPULATED AND AGREED by and between the parties, through their respective counsel, subject to the approval of the Court, that a

Protective Order pursuant to Rule 26(c) of the Federal Rules of Civil Procedure be entered as follows.

IT IS ORDERED THAT:

1. This Protective Order shall apply to all information, documents, electronic documents, things, discovery responses and testimony designated in good faith as constituting or containing confidential material by parties and non-parties in this litigation. Any confidential material produced by a party or non-party in this litigation may be designated by such party or non-party as (1) "CONFIDENTIAL" or (2) "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under the terms of this Protective Order.

2. For the purposes of this Protective Order, confidential material designated as "CONFIDENTIAL" shall be information or tangible things that the producing party believes in good faith qualifies for protection under standards developed under Rule 26(c) of the Federal Rules of Civil Procedure, including trade secrets or other confidential research, development, commercial or business information. Absent a specific order by this Court, once designated as “CONFIDENTIAL” such designated confidential material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such information shall not be disclosed to anyone except as provided herein.

3. Confidential material designated as “HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY” shall be information that the producing party believes in good faith is extremely sensitive confidential information whose disclosure to another

party or non-party would create a substantial adverse impact on the producing party's business, financial condition, ability to compete, standing in the industry or any other risk of injury that could not be avoided by less restrictive means. Such material includes, without limitation, information related to confidential technical or product information not released to the public; future projections, strategies, forecasts, or business plans; company financial information or financial analyses and projections that have not been made public; contractual relationships with third parties; identification of customers and vendors, materials relating to ongoing research and development efforts and future products; technical materials used solely for internal purposes in connection with development, production, engineering, or sales training; source code; and documents relating to the prosecution of patents that have not been issued and contain claims that are not publicly known. Absent a specific order by this Court, once designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," such designated material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such material shall not be disclosed to anyone except as provided herein.

4. Each party or nonparty that designates confidential material for protection under this Protective Order must take care to limit any such designation to specific material that qualifies under the appropriate standards. Mass, indiscriminate and routinized designations are prohibited. The designation of confidential material as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY"

for purposes of this Protective Order shall be made in the following manner by the party or non-party seeking protection:

(a) in the case of documents, electronic documents, exhibits, briefs, memoranda, interrogatory responses, responses to requests for admission, things or other materials (apart from depositions, pretrial or trial testimony): by affixing the legend "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, to every page of any document containing confidential material at the time such documents are produced or such information is disclosed, or as soon thereafter as the party or non-party seeking protection becomes aware of the confidential nature of the material disclosed and sought to be protected; and

(b) in the case of depositions, pretrial and trial testimony: (i) by a statement by counsel on the record during such deposition, pretrial or trial proceeding that the entire transcript or a portion thereof shall be designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, hereunder; or (ii) by written notice of such designation sent by counsel to all parties within twenty (20) calendar days of its receipt of the transcript of the testimony. The parties shall treat all deposition, pretrial and trial testimony as "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" hereunder until the expiration of twenty (20) calendar days of the receipt of the transcript. Unless so designated, any confidentiality is waived after the expiration of the 20-day period unless otherwise stipulated or ordered. The parties may modify this procedure for any particular

deposition or proceeding through agreement on the record at such deposition or proceeding or otherwise by written stipulation, without further order of the Court.

If confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" is used during the course of a deposition, that portion of the deposition record reflecting such confidential material shall be sealed and stamped with the designated degree of confidentiality, and access thereto shall be limited pursuant to the other terms of this Protective Order.

5. Confidential material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) Outside counsel for the parties identified as follows:

(1) For Plaintiff Secure Computing Corporation: Robins, Kaplan, Miller & Ciresi LLP.

(2) For Defendants Finjan Software, Ltd. and Finjan Software, Inc.: Perkins Coie LLP and Merchant & Gould P.C.

(3) As used herein, "outside counsel" shall mean attorneys for the respective firms, including supporting personnel employed by the attorneys, such as patent agents, paralegals, legal secretaries, legal clerks, and litigation support employees who are not presently involved in patent prosecution related to the subject matter of this litigation and will not be involved in *ex*

parte patent prosecution related to the subject matter of this litigation for three years following disclosure of the confidential material – this shall not preclude the recipient of confidential material from participating in *inter partes* or contested proceedings in a patent office.

(b) officers, directors and employees of the parties whose assistance is needed by counsel for the purposes of this litigation;

(c) no more than three individuals who serve as in-house counsel of each party where the assistance of that individual is needed by that party's counsel for the purposes of this litigation provided that for each individual provided access to material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof pursuant to this subsection, the party:

(1) provide the identity of the individual to all other parties in writing; and

(2) have the identified confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. A receiving party's outside counsel shall retain any such executed confidentiality agreements, and they need not be disclosed to the producing party unless the producing party, for good cause, requests a copy of such agreement(s).

(d) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(e) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(f) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(g) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(h) non-technical jury or trial consulting services retained by counsel for a party;

(i) the author(s) and all recipients of the document or the original source of the information; and

(j) any other person only upon order of the Court or upon written consent of the party producing the confidential material, subject to and conditioned upon compliance with Paragraph 8 herein.

6. Confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) parties' outside counsel of record in this litigation, as defined in paragraph 5(a) above;

(b) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(c) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(d) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(e) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(f) non-technical jury or trial consulting services retained by counsel for a party;

(g) any other person only upon order of the Court or upon written consent of the party producing the confidential information or material subject to and conditioned upon compliance with Paragraph 8 herein.

7. For purposes of Paragraphs 5(c) and 6(b) herein, a consultant or expert shall be defined as a person who is neither an employee, agent or representative of a party, nor anticipated to become an employee, agent or representative of a party in the near future, and who is retained or employed to assist in the preparation for trial in this litigation, whether full or part time, by or at the direction of counsel for a party. The procedure for having a consultant or expert approved for access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" shall be as follows:

(a) Outside counsel for the receiving party shall (i) provide the individual with a copy of this Protective Order, (2) explain its terms, and (3) obtain the

individual's written agreement, in the form of Exhibit A hereto, to comply with and be bound by its terms. Within five (5) court days of signing Exhibit A, the receiving party must identify in writing the individual to the producing party and provide the producing party with an executed Exhibit A and a written statement setting forth that person's present residence address, business address, employer, job title, any past or present association with any party, any litigation that the individual has provided any professional services during the preceding five years, and a current curriculum vitae;

(b) The receiving party that sends the identification specified in the preceding paragraph may disclose confidential material to the identified individual unless, within five (5) court days of delivering the identification, the party receives a written objection, served by facsimile or electronic mail, to the identification, setting forth in detail the grounds on which it is based. If a party receives such an objection, the individual shall be barred from access to the confidential material for a fourteen (14) calendar day period commencing with the receipt by the producing party of a copy of the executed Exhibit A;

(c) If within that fourteen (14) calendar day period, the parties are unable to resolve their differences and the opposing party moves for a further protective order, then the confidential material shall not be provided to said individual except by further order of the Court. Any such motion must describe the circumstances with specificity, set forth in detail the reasons for which the disclosure is reasonably necessary, assess the risk of harm that the disclosure would entail, and suggest any additional means that might be used to reduce that risk. The party opposing the disclosure to said

individual shall bear the burden of proving that the risk of harm that the disclosure would entail (under the safeguards proposed) outweighs the seeking party's need to disclose the confidential material to said individual.

8. All persons listed in Paragraphs 5(b), 5(f), and 5(g), above, and interpreters or translators referenced in Paragraph 5(e), may be given access to confidential material designated as "CONFIDENTIAL," provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. Similarly, all persons listed in Paragraphs 6(e) and 6(f) above, and interpreters or translators referenced in Paragraph 6(e), may be given access to confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A.

9. Any person may be examined as a witness at trial or during a deposition concerning any confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" which that person had lawfully received or authored prior to and apart from this litigation. During examination, any such witness may be shown confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by a party that appears on its face, or from other documents or testimony, to have been received from or authored by that witness or communicated to that witness. .

10. Confidential material may be filed with or presented to the Court, or may be included in briefs, memoranda or other papers filed with this Court, but if so, they shall be filed under seal in accordance with the Local Rules of the Court and the United States District Court for the District of Minnesota.

11. A party may challenge any other party's designation of confidential materials produced herein as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by serving a written objection upon the producing party. A party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed. In the event that a party challenges in writing, at any time during this litigation, the designation of confidential material, the designating party, shall, within fourteen (14) calendar days of such challenge, substantiate the basis for such designation in writing. If no substantiation is proffered, the material shall not be deemed designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order. If substantiation is offered, the parties shall first try to resolve such dispute in good faith on an informal basis. If the dispute cannot be resolved, the party challenging the claim of confidentiality may seek appropriate relief from the Court. Each such motion shall identify the challenged material and the basis for the challenge. Until a dispute over the asserted designation is finally resolved by the parties or the Court, all parties and persons shall treat the confidential material in question as designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY."

12. All counsel for the parties who have access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order acknowledge they are bound by this Order and submit to the jurisdiction of this Court for purposes of enforcing this Order.

13. Entering into, agreeing to, and/or producing or receiving confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or otherwise complying with the terms of this Protective Order shall not:

(a) waive any right to object on any ground to use in evidence of any of the confidential material covered by this Protective Order;

(b) waive any objection otherwise available to the disclosure or production of confidential material on any ground not addressed in this Protective Order.

14. This Protective Order has no effect upon, and shall not apply to, a party's use or disclosure of its own confidential material for any purpose. Nothing contained herein shall impose any restrictions on the use or disclosure by a party of confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" obtained lawfully by such party independently of any proceedings in this action, or which:

(a) was already known to such party by lawful means prior to acquisition from, or disclosure by, any other party in this action;

(b) is or becomes publicly known through no fault or act of such party; or

(c) is rightfully received by such party from a third party that has authority to provide such information or material and without restriction as to disclosure.

15. If a party inadvertently produces "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" material without marking it as such, it may be disclosed to others until the receiving party becomes aware of the error, unless it appears from the face of the document that it contains non-public, confidential, proprietary, commercially sensitive, or trade secret information of the producing party. As soon as the receiving party becomes aware of the inadvertent production, the information must be treated as if it had been timely designated under this Protective Order, and the receiving party must endeavor in good faith to obtain all copies of the material that it distributed or disclosed to persons not authorized to access such information by Paragraphs 5 and 6 above, as well as any copies made by such persons. If timely corrected, an inadvertent failure to designate confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" does not, standing alone, waive the producing party's right to secure protection under this Protective Order for such material.

16. If a party learns that, by inadvertence or otherwise, it has disclosed confidential material to any person or in any circumstance not authorized under this Protective Order, that party must immediately (1) notify in writing the designating party of the unauthorized disclosures, (2) use its best efforts to retrieve all copies of the confidential material, (3) inform the person or persons to whom unauthorized disclosures

were made of all the terms of this Order, and (4) request such person or persons complete and sign a copy of the undertaking in the form attached hereto as Exhibit A.

17. The production of confidential material which are alleged to have been inadvertently produced and are subject to the attorney client privilege, work product immunity or other protection from disclosure, shall not constitute a waiver of such privilege. After receiving notice from the producing party that confidential material subject to protection has been inadvertently produced, the receiving party shall not review, copy or disseminate such confidential material. The receiving party shall return such confidential material to the producing party immediately. Return of the confidential material by the receiving party shall not constitute an admission or concession, or permit any inference, that the returned material is, in fact, properly subject to a claim of attorney-client privilege, work product immunity, or other protection from disclosure, nor shall it foreclose any party from moving the Court for an order that such material has been improperly designated or should be discoverable and/or usable in this litigation for reasons other than a waiver caused by the inadvertent production.

18. It is the present intention of the parties that the provisions of this Protective Order shall govern discovery and other pretrial and trial proceedings in this action. Nonetheless, each of the parties hereto shall be entitled to seek modification of this Protective Order by application to the Court on notice to the other parties hereto for good cause.

19. The provisions of this Protective Order shall, absent written permission of the producing party or further order of the Court, continue to be binding throughout and

after the conclusion of this action, including without limitation any appeals therefrom. Within sixty (60) calendar days after receiving notice of the entry of an order, judgment, or decree finally disposing of this action, including any appeals therefrom, all persons having received confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" hereunder shall return such material and all copies thereof (including summaries and excerpts) to counsel for the producing party, or shall certify destruction thereof. Counsel described in paragraphs 5(a) and 6(a) above shall be entitled to retain court papers, deposition and trial transcripts, and attorney work product (including court papers, transcripts, and attorney work product that contain information or material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY") and to one copy of documents produced by the opposing party designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that such counsel, and employees of such counsel, shall not disclose any such information and material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" contained in such court papers, transcripts, attorney work product, or documents to any person or entity except pursuant to a written agreement with the producing party of the information or material. Within 60 days following the expiration of the last period for appeal from any order issued in connection with this action, the parties shall remove any materials designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" from the office of the Clerk of Court. Following that 60-day period, the Clerk of Court shall destroy all designated

"CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" materials.

20. If any party (a) is subpoenaed in another action, (b) is served with a demand in another action to which it is a party, or (c) is served with any other legal process by one not a party to this litigation, seeking information or material which was produced or designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by someone other than that party, the party shall give prompt actual written notice no more than five (5) court days of receipt of such subpoena, demand, or legal process, to those who produced or designated the confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" and shall object to its production to the extent permitted by law. Should the person seeking access to the confidential material take action against the party or anyone else covered by this Protective Order to enforce such a subpoena, demand or other legal process, the party shall respond by setting forth the existence of this Protective Order. The designating party shall bear the burdens and the expenses of seeking protection in that court of its confidential material, and nothing in these provisions should be construed as authorizing or encouraging a party in this action to disobey a lawful directive from another court.

21. The parties agree that all designated documents, information, and material exchanged between the parties and subject to this Protective Order in this action shall be used solely for the prosecution or defense of the claims in this action and shall not be

used for any business, commercial, competitive, personal, or other purposes, subject to the other terms of this Protective Order.

22. Nothing in this Protective Order shall prevent outside or inside counsel from giving legal advice based on information that has been designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided such legal advice shall not reveal the substance of any designated information to a person who is not authorized to receive it.

23. The parties agree to be bound by the terms of this Protective Order pending its entry by the Court, or pending the entry of an alternative thereto which is satisfactory to all parties, and any violation of its terms shall be subject to the same sanctions and penalties as if the Protective Order had been entered by the Court.

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: _____/s/ Christopher A. Seidl_____
Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (#313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Attorneys for Plaintiff
Secure Computing Corp.

MERCHANT & GOULD P.C.

By: ___/s/ Anthony R. Zeuli_____
Anthony R. Zeuli (#274884)
J.R. Maddox, (#329523)
3200 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
(612) 332-5300

Of Counsel:

Paul J. Andre
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114
(650) 838-4300

Attorneys for Defendants
Finjan Software, Ltd., and Finjan Software, Inc.

SO ORDERED, this ____ day of _____, 2007

_____
United States District Judge

Exhibit A
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)))))))))	Civil Action No. 07-CV-2198 JMR/FLN

STIPULATED PROTECTIVE ORDER

UNDERTAKING OF: _____

1. My home address is:

2. My present employer is and the address of my present employment is:

3. My present occupation or job description is:

4. I have received a copy of the Stipulated Protective Order in this litigation.

5. I have carefully read and understand the provisions of the Stipulated Protective Order in this litigation.

6. I will comply with all of the provisions of the Stipulated Protective Order.

7. I will hold in confidence, will not disclose to anyone not qualified under the Stipulated Protective Order, and will use only for purposes of this litigation, in strict compliance with the terms and conditions of the Stipulated Protective Order, any confidential material which is disclosed to me. I acknowledge that termination of the litigation does not release me from the obligations set out in this paragraph.

8. I will return all confidential information which comes into my possession, and documents or things which I have prepared relating thereto, to counsel for the party

by whom I am employed or retained in strict accordance with the provisions of the Stipulated Protective Order.

9. I hereby submit to the jurisdiction of this Court for the purposes of enforcement of the Stipulated Protective Order in this litigation.

10. Any accompanying resume or curriculum vitae is a complete and accurate statement to the best of my knowledge, and I acknowledge that in submitting such resume or curriculum vitae I know that the receiving party shall rely thereon.

11. I make the above statements under penalty of perjury.

Signature:_____
Date:_____

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.

Defendants.

Case No. 0:07-cv-2198 JMR/FLN

CERTIFICATE OF SERVICE

I hereby certify that on the 24th day of July, 2007, I caused the following document:

AMENDED STIPULATED PROTECTIVE ORDER

to be filed electronically with the Clerk of Court through ECF, and that ECF will send an e-notice of the electronic filing to the following counsel of record:

Anthony R. Zeuli tzeuli@merchant-gould.com

I further certify that a courtesy copy was delivered to Chief Judge James M. Rosenbaum's chambers, and that the Amended Stipulated Protective Order was filed with the court via e-mail to the following judge:

Chief Judge James M. Rosenbaum rosenbaum_chambers@mnd.uscourts.gov

I certify that a copy of the Amended Stipulated Protective Order was served on counsel via e-mail as follows:

Anthony R. Zeuli tzeuli@merchant-gould.com
James Hannah jhannah@perkinscoie.com

Dated: July 24, 2007 By: s/Christopher A. Seidl

UNITED STATES DISTRICT COURT

Clear Form

District of Minnesota

MOTION FOR ADMISSION PRO HAC VICE

Case Number: 07-CV-02198 **Case Title:** Secure Computing Corporation v. Finjan Software Ltd.

Affidavit of Movant

I, Anthony R. Zeuli, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota, request that this Court admit pro hac vice Paul Joseph Andre, an attorney admitted to practice and currently in good standing in the U.S. District Court for the Northern District of California, but not admitted to the bar of this court, who will be counsel for the ☐ plaintiff ☑ defendant Finjan Software Ltd in the case listed above. I am aware that the local rules of this court require that an active Minnesota resident member in good standing participate in the preparation and presentation of the case listed above, and accept service of all papers served.

Check one of the following:

☑ 1. I am a resident of the State of Minnesota, and will participate and accept service as required by LR 83.5(d).
☐ 2. I am not a resident of the State of Minnesota.
☐ 3. I am a resident of the State of Minnesota, but will not participate and accept service as required by LR 83.5(d).

Signature : s/Anthony R. Zeuli	0274884	07/24/07
Typed Name: Anthony R. Zeuli	MN Attorney License #	Date

Affidavit of Resident Minnesota Bar Member (Required **ONLY if movant checks box 2 or 3 above**.)

I, _____, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota and a resident of the State of Minnesota, agree to participate in the preparation and presentation of the case listed above, and accept service of all papers served as required by LR 83.5(d).

Signature : _____	_____	_____
Typed Name: _____	MN Attorney License #	Date

Affidavit of Proposed Admittee

I, Paul Joseph Andre, am currently a member in good standing of the U.S. District Court for the Northern District of California, but am not admitted to the bar of this court. I understand that if this Court grants me admission pro hac vice, the resident attorney identified in this motion must participate in the preparation and presentation of the case listed above, and must accept service of all papers served as required by LR 83.5(d). I further understand that the District of Minnesota is an electronic court and that I consent to service required by Fed.R.Civ.P. 77 by electronic means and I understand that electronic notice will be in lieu of service by mail unless the Court learns that a failure has occurred in which case service will be effected by mail within 24 hours.

Paul Joseph Andre	s/Paul Joseph Andre	07/06/07
Type/Print Name (must match name above)	Signature	Date

Attorney License Number: 196585 issued by the State of CA (initials)

Law Firm Name: Perkins Coie LLP Main Phone: (650) 838-4300

Law Firm Addrs: 101 Jefferson Drive Direct Phone: (650) 838-4370

Menlo Park, CA 94025 E-mail Addrs: PAndre@perkinscoie.com

Note: This page shall be converted to PDF and e-filed in ECF - do not e-file first page. A check in the amount of the Pro Hac Vice admission fee of $100 shall be mailed or delivered to the Admissions Clerk or a Credit Card Authorization form shall be faxed to the Admissions Clerk before you will be included in the roll of admitted attorneys and receive notices generated in the above-entitled action.

UNITED STATES DISTRICT COURT

Clear Form

District of Minnesota

MOTION FOR ADMISSION PRO HAC VICE

Case Number: 07-CV-02198 **Case Title:** Secure Computing Corporation v. Finjan Software Ltd.

Affidavit of Movant

I, Anthony R. Zeuli, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota, request that this Court admit pro hac vice Lisa Kobialka, an attorney admitted to practice and currently in good standing in the U.S. District Court for the Northern District of California, but not admitted to the bar of this court, who will be counsel for the ☐ plaintiff ☑ defendant Finjan Software Ltd in the case listed above. I am aware that the local rules of this court require that an active Minnesota resident member in good standing participate in the preparation and presentation of the case listed above, and accept service of all papers served.

Check one of the following:

☑ 1. I am a resident of the State of Minnesota, and will participate and accept service as required by LR 83.5(d).
☐ 2. I am not a resident of the State of Minnesota.
☐ 3. I am a resident of the State of Minnesota, but will not participate and accept service as required by LR 83.5(d).

Signature : s/Anthony R. Zeuli	0274884	07/24/07
Typed Name: Anthony R. Zeuli	MN Attorney License #	Date

Affidavit of Resident Minnesota Bar Member (Required **ONLY if movant checks box 2 or 3 above**.)

I, _____, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota and a resident of the State of Minnesota, agree to participate in the preparation and presentation of the case listed above, and accept service of all papers served as required by LR 83.5(d).

Signature : _____	_____	_____
Typed Name: _____	MN Attorney License #	Date

Affidavit of Proposed Admittee

I, Lisa Kobialka, am currently a member in good standing of the U.S. District Court for the Northern District of California, but am not admitted to the bar of this court. I understand that if this Court grants me admission pro hac vice, the resident attorney identified in this motion must participate in the preparation and presentation of the case listed above, and must accept service of all papers served as required by LR 83.5(d). I further understand that the District of Minnesota is an electronic court and that I consent to service required by Fed.R.Civ.P. 77 by electronic means and I understand that electronic notice will be in lieu of service by mail unless the Court learns that a failure has occurred in which case service will be effected by mail within 24 hours.

Lisa Kobialka	s/Lisa Kobialka	07/10/07
Type/Print Name (must match name above)	Signature	Date

Attorney License Number: 191404 issued by the State of CA (initials)

Law Firm Name: Perkins Coie LLP Main Phone: (650) 838-4300

Law Firm Addrs: 101 Jefferson Drive Direct Phone: (650) 838-4447

Menlo Park, CA 94025 E-mail Addrs: LKobialka@perkinscoie.com

Note: This page shall be converted to PDF and e-filed in ECF - do not e-file first page. A check in the amount of the Pro Hac Vice admission fee of $100 shall be mailed or delivered to the Admissions Clerk or a Credit Card Authorization form shall be faxed to the Admissions Clerk before you will be included in the roll of admitted attorneys and receive notices generated in the above-entitled action.

UNITED STATES DISTRICT COURT

Clear Form

District of Minnesota

MOTION FOR ADMISSION PRO HAC VICE

Case Number: 07-CV-02198 **Case Title:** Secure Computing Corporation v. Finjan Software Ltd.

Affidavit of Movant

I, Anthony R. Zeuli, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota, request that this Court admit pro hac vice James R. Hannah, an attorney admitted to practice and currently in good standing in the U.S. District Court for the Northern District of California, but not admitted to the bar of this court, who will be counsel for the ☐ plaintiff ☑ defendant Finjan Software Ltd in the case listed above. I am aware that the local rules of this court require that an active Minnesota resident member in good standing participate in the preparation and presentation of the case listed above, and accept service of all papers served.

Check one of the following:

☑ 1. I am a resident of the State of Minnesota, and will participate and accept service as required by LR 83.5(d).
☐ 2. I am not a resident of the State of Minnesota.
☐ 3. I am a resident of the State of Minnesota, but will not participate and accept service as required by LR 83.5(d).

Signature : s/Anthony R. Zeuli	0274884	07/24/07
Typed Name: Anthony R. Zeuli	MN Attorney License #	Date

Affidavit of Resident Minnesota Bar Member (Required **ONLY if movant checks box 2 or 3 above**.)

I, _____, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota and a resident of the State of Minnesota, agree to participate in the preparation and presentation of the case listed above, and accept service of all papers served as required by LR 83.5(d).

Signature : _____	_____	_____
Typed Name: _____	MN Attorney License #	Date

Affidavit of Proposed Admittee

I, James R. Hannah, am currently a member in good standing of the U.S. District Court for the Northern District of California, but am not admitted to the bar of this court. I understand that if this Court grants me admission pro hac vice, the resident attorney identified in this motion must participate in the preparation and presentation of the case listed above, and must accept service of all papers served as required by LR 83.5(d). I further understand that the District of Minnesota is an electronic court and that I consent to service required by Fed.R.Civ.P. 77 by electronic means and I understand that electronic notice will be in lieu of service by mail unless the Court learns that a failure has occurred in which case service will be effected by mail within 24 hours.

James R. Hannah	s/James R. Hannah	07/11/07
Type/Print Name (must match name above)	Signature	Date

Attorney License Number: 237978 issued by the State of CA (initials)

Law Firm Name: Perkins Coie LLP Main Phone: (650) 838-4300

Law Firm Addrs: 101 Jefferson Drive Direct Phone: (650) 838-4307

Menlo Park, CA 94025 E-mail Addrs: JHannah@perkinscoie.com

Note: This page shall be converted to PDF and e-filed in ECF - do not e-file first page. A check in the amount of the Pro Hac Vice admission fee of $100 shall be mailed or delivered to the Admissions Clerk or a Credit Card Authorization form shall be faxed to the Admissions Clerk before you will be included in the roll of admitted attorneys and receive notices generated in the above-entitled action.

UNITED STATES DISTRICT COURT

Clear Form

District of Minnesota

MOTION FOR ADMISSION PRO HAC VICE

Case Number: 07-CV-02198 **Case Title:** Secure Computing Corporation v. Finjan Software Ltd.

Affidavit of Movant

I, Anthony R. Zeuli, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota, request that this Court admit pro hac vice Meghan Ashley Wharton, an attorney admitted to practice and currently in good standing in the U.S. District Court for the District of Arizona, but not admitted to the bar of this court, who will be counsel for the ☐ plaintiff ☑ defendant Finjan Software Ltd in the case listed above. I am aware that the local rules of this court require that an active Minnesota resident member in good standing participate in the preparation and presentation of the case listed above, and accept service of all papers served.

Check one of the following:

☑ 1. I am a resident of the State of Minnesota, and will participate and accept service as required by LR 83.5(d).
☐ 2. I am not a resident of the State of Minnesota.
☐ 3. I am a resident of the State of Minnesota, but will not participate and accept service as required by LR 83.5(d).

Signature : s/Anthony R. Zeuli	0274884	07/24/07
Typed Name: Anthony R. Zeuli	MN Attorney License #	Date

Affidavit of Resident Minnesota Bar Member (Required **ONLY if movant checks box 2 or 3 above**.)

I, _____, an active member in good standing of the bar of the U.S. District Court for the District of Minnesota and a resident of the State of Minnesota, agree to participate in the preparation and presentation of the case listed above, and accept service of all papers served as required by LR 83.5(d).

Signature : _____	_____	_____
Typed Name: _____	MN Attorney License #	Date

Affidavit of Proposed Admittee

I, Meghan Ashley Wharton, am currently a member in good standing of the U.S. District Court for the District of Arizona, but am not admitted to the bar of this court. I understand that if this Court grants me admission pro hac vice, the resident attorney identified in this motion must participate in the preparation and presentation of the case listed above, and must accept service of all papers served as required by LR 83.5(d). I further understand that the District of Minnesota is an electronic court and that I consent to service required by Fed.R.Civ.P. 77 by electronic means and I understand that electronic notice will be in lieu of service by mail unless the Court learns that a failure has occurred in which case service will be effected by mail within 24 hours.

Meghan Ashley Wharton	s/Meghan Wharton	07/24/07
Type/Print Name (must match name above)	Signature	Date

Attorney License Number: 020955 issued by the State of AZ (initials)

Law Firm Name: Perkins Coie LLP Main Phone: (650) 838-4300

Law Firm Addrs: 101 Jefferson Drive Direct Phone: (650) 838-4363

Menlo Park, CA 94025 E-mail Addrs: mwharton@perkinscoie.com

Note: This page shall be converted to PDF and e-filed in ECF - do not e-file first page. A check in the amount of the Pro Hac Vice admission fee of $100 shall be mailed or delivered to the Admissions Clerk or a Credit Card Authorization form shall be faxed to the Admissions Clerk before you will be included in the roll of admitted attorneys and receive notices generated in the above-entitled action.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)	Civil Action No. 07-CV-2198 JMR/FLN

AMENDED STIPULATED PROTECTIVE ORDER

WHEREAS, discovery in the above entitled litigation may involve the disclosure of confidential trade secret, technical know-how, or other confidential or proprietary research, development, commercial, personal, financial information or information furnished in confidence by a third party (hereinafter individually and collectively referred to as "confidential material") relating to the subject matter of this litigation, regardless of how generated;

WHEREAS, the parties desire to limit the extent of disclosure and use of such confidential material, and to protect such confidential material from unauthorized use and/or further disclosure, and wish to insure that no advantage is gained by any party by the use of such confidential material which could not have been learned had discovery in this litigation has not occurred.

NOW, THEREFORE, IT IS STIPULATED AND AGREED by and between the parties, through their respective counsel [Docket No. 17], and APPROVED by the Court,

that a Protective Order pursuant to Rule 26(c) of the Federal Rules of Civil Procedure be entered as follows.

IT IS ORDERED THAT:

1. This Protective Order shall apply to all information, documents, electronic documents, things, discovery responses and testimony designated in good faith as constituting or containing confidential material by parties and non-parties in this litigation. Any confidential material produced by a party or non-party in this litigation may be designated by such party or non-party as (1) "CONFIDENTIAL" or (2) "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under the terms of this Protective Order.

2. For the purposes of this Protective Order, confidential material designated as "CONFIDENTIAL" shall be information or tangible things that the producing party believes in good faith qualifies for protection under standards developed under Rule 26(c) of the Federal Rules of Civil Procedure, including trade secrets or other confidential research, development, commercial or business information. Absent a specific order by this Court, once designated as "CONFIDENTIAL" such designated confidential material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such information shall not be disclosed to anyone except as provided herein.

3. Confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" shall be information that the producing party believes in good faith is extremely sensitive confidential information whose disclosure to another

party or non-party would create a substantial adverse impact on the producing party's business, financial condition, ability to compete, standing in the industry or any other risk of injury that could not be avoided by less restrictive means. Such material includes, without limitation, information related to confidential technical or product information not released to the public; future projections, strategies, forecasts, or business plans; company financial information or financial analyses and projections that have not been made public; contractual relationships with third parties; identification of customers and vendors, materials relating to ongoing research and development efforts and future products; technical materials used solely for internal purposes in connection with development, production, engineering, or sales training; source code; and documents relating to the prosecution of patents that have not been issued and contain claims that are not publicly known. Absent a specific order by this Court, once designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," such designated material shall be used by the parties solely in connection with this litigation, and not for any business, competitive, or governmental purpose or function, and such material shall not be disclosed to anyone except as provided herein.

4. Each party or nonparty that designates confidential material for protection under this Protective Order must take care to limit any such designation to specific material that qualifies under the appropriate standards. Mass, indiscriminate and routinized designations are prohibited. The designation of confidential material as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY"

for purposes of this Protective Order shall be made in the following manner by the party or non-party seeking protection:

(a) in the case of documents, electronic documents, exhibits, briefs, memoranda, interrogatory responses, responses to requests for admission, things or other materials (apart from depositions, pretrial or trial testimony): by affixing the legend "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, to every page of any document containing confidential material at the time such documents are produced or such information is disclosed, or as soon thereafter as the party or non-party seeking protection becomes aware of the confidential nature of the material disclosed and sought to be protected; and

(b) in the case of depositions, pretrial and trial testimony: (i) by a statement by counsel on the record during such deposition, pretrial or trial proceeding that the entire transcript or a portion thereof shall be designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," as appropriate, hereunder; or (ii) by written notice of such designation sent by counsel to all parties within twenty (20) calendar days of its receipt of the transcript of the testimony. The parties shall treat all deposition, pretrial and trial testimony as "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" hereunder until the expiration of twenty (20) calendar days of the receipt of the transcript. Unless so designated, any confidentiality is waived after the expiration of the 20-day period unless otherwise stipulated or ordered. The parties may modify this procedure for any particular

deposition or proceeding through agreement on the record at such deposition or proceeding or otherwise by written stipulation, without further order of the Court.

If confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" is used during the course of a deposition, that portion of the deposition record reflecting such confidential material shall be sealed and stamped with the designated degree of confidentiality, and access thereto shall be limited pursuant to the other terms of this Protective Order.

5. Confidential material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) Outside counsel for the parties identified as follows:

(1) For Plaintiff Secure Computing Corporation: Robins, Kaplan, Miller & Ciresi LLP.

(2) For Defendants Finjan Software, Ltd. and Finjan Software, Inc.: Perkins Coie LLP and Merchant & Gould P.C.

(3) As used herein, "outside counsel" shall mean attorneys for the respective firms, including supporting personnel employed by the attorneys, such as patent agents, paralegals, legal secretaries, legal clerks, and litigation support employees who are not presently involved in patent prosecution related to the subject matter of this litigation and will not be involved in *ex*

parte patent prosecution related to the subject matter of this litigation for three years following disclosure of the confidential material – this shall not preclude the recipient of confidential material from participating in *inter partes* or contested proceedings in a patent office.

(b) officers, directors and employees of the parties whose assistance is needed by counsel for the purposes of this litigation;

(c) no more than three individuals who serve as in-house counsel of each party where the assistance of that individual is needed by that party's counsel for the purposes of this litigation provided that for each individual provided access to material designated as "CONFIDENTIAL," or copies or extracts therefrom and compilations and summaries thereof pursuant to this subsection, the party:

(1) provide the identity of the individual to all other parties in writing; and

(2) have the identified confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. A receiving party's outside counsel shall retain any such executed confidentiality agreements, and they need not be disclosed to the producing party unless the producing party, for good cause, requests a copy of such agreement(s).

(d) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(e) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(f) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(g) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(h) non-technical jury or trial consulting services retained by counsel for a party;

(i) the author(s) and all recipients of the document or the original source of the information; and

(j) any other person only upon order of the Court or upon written consent of the party producing the confidential material, subject to and conditioned upon compliance with Paragraph 8 herein.

6. Confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or copies or extracts therefrom and compilations and summaries thereof, may be disclosed, summarized, described, characterized, or otherwise communicated or made available in whole or in part only to the following persons:

(a) parties' outside counsel of record in this litigation, as defined in paragraph 5(a) above;

(b) consultants and experts as defined in and pursuant to the provisions of Paragraph 7 herein;

(c) the Court and those employed by the Court, pursuant to Paragraph 10 herein;

(d) court reporters, videographers, outside copying, interpreters or translators, employed in connection with this litigation;

(e) graphics or design services retained by counsel for a party for purposes of preparing demonstrative or other exhibits for deposition, trial, or other court proceedings in this litigation;

(f) non-technical jury or trial consulting services retained by counsel for a party;

(g) any other person only upon order of the Court or upon written consent of the party producing the confidential information or material subject to and conditioned upon compliance with Paragraph 8 herein.

7. For purposes of Paragraphs 5(c) and 6(b) herein, a consultant or expert shall be defined as a person who is neither an employee, agent or representative of a party, nor anticipated to become an employee, agent or representative of a party in the near future, and who is retained or employed to assist in the preparation for trial in this litigation, whether full or part time, by or at the direction of counsel for a party. The procedure for having a consultant or expert approved for access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL– ATTORNEYS' EYES ONLY" shall be as follows:

(a) Outside counsel for the receiving party shall (i) provide the individual with a copy of this Protective Order, (2) explain its terms, and (3) obtain the

individual's written agreement, in the form of Exhibit A hereto, to comply with and be bound by its terms. Within five (5) court days of signing Exhibit A, the receiving party must identify in writing the individual to the producing party and provide the producing party with an executed Exhibit A and a written statement setting forth that person's present residence address, business address, employer, job title, any past or present association with any party, any litigation that the individual has provided any professional services during the preceding five years, and a current curriculum vitae;

(b) The receiving party that sends the identification specified in the preceding paragraph may disclose confidential material to the identified individual unless, within five (5) court days of delivering the identification, the party receives a written objection, served by facsimile or electronic mail, to the identification, setting forth in detail the grounds on which it is based. If a party receives such an objection, the individual shall be barred from access to the confidential material for a fourteen (14) calendar day period commencing with the receipt by the producing party of a copy of the executed Exhibit A;

(c) If within that fourteen (14) calendar day period, the parties are unable to resolve their differences and the opposing party moves for a further protective order, then the confidential material shall not be provided to said individual except by further order of the Court. Any such motion must describe the circumstances with specificity, set forth in detail the reasons for which the disclosure is reasonably necessary, assess the risk of harm that the disclosure would entail, and suggest any additional means that might be used to reduce that risk. The party opposing the disclosure to said

individual shall bear the burden of proving that the risk of harm that the disclosure would entail (under the safeguards proposed) outweighs the seeking party's need to disclose the confidential material to said individual.

8. All persons listed in Paragraphs 5(b), 5(f), and 5(g), above, and interpreters or translators referenced in Paragraph 5(e), may be given access to confidential material designated as "CONFIDENTIAL," provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A. Similarly, all persons listed in Paragraphs 6(e) and 6(f) above, and interpreters or translators referenced in Paragraph 6(e), may be given access to confidential material designated as "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that they first confirm their understanding and agreement to abide by the terms of this Protective Order by completing and signing a copy of an undertaking in the form attached hereto as Exhibit A.

9. Any person may be examined as a witness at trial or during a deposition concerning any confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" which that person had lawfully received or authored prior to and apart from this litigation. During examination, any such witness may be shown confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by a party that appears on its face, or from other documents or testimony, to have been received from or authored by that witness or communicated to that witness. .

10. Confidential material may be filed with or presented to the Court, or may be included in briefs, memoranda or other papers filed with this Court, but if so, they shall be filed under seal in accordance with the Local Rules of the Court and the United States District Court for the District of Minnesota.

11. A party may challenge any other party's designation of confidential materials produced herein as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by serving a written objection upon the producing party. A party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed. In the event that a party challenges in writing, at any time during this litigation, the designation of confidential material, the designating party, shall, within fourteen (14) calendar days of such challenge, substantiate the basis for such designation in writing. If no substantiation is proffered, the material shall not be deemed designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order. If substantiation is offered, the parties shall first try to resolve such dispute in good faith on an informal basis. If the dispute cannot be resolved, the party challenging the claim of confidentiality may seek appropriate relief from the Court. Each such motion shall identify the challenged material and the basis for the challenge. Until a dispute over the asserted designation is finally resolved by the parties or the Court, all parties and persons shall treat the confidential material in question as designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY."

12. All counsel for the parties who have access to confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under this Protective Order acknowledge they are bound by this Order and submit to the jurisdiction of this Court for purposes of enforcing this Order.

13. Entering into, agreeing to, and/or producing or receiving confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY," or otherwise complying with the terms of this Protective Order shall not:

(a) waive any right to object on any ground to use in evidence of any of the confidential material covered by this Protective Order;

(b) waive any objection otherwise available to the disclosure or production of confidential material on any ground not addressed in this Protective Order.

14. This Protective Order has no effect upon, and shall not apply to, a party's use or disclosure of its own confidential material for any purpose. Nothing contained herein shall impose any restrictions on the use or disclosure by a party of confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" obtained lawfully by such party independently of any proceedings in this action, or which:

(a) was already known to such party by lawful means prior to acquisition from, or disclosure by, any other party in this action;

(b) is or becomes publicly known through no fault or act of such party; or

(c) is rightfully received by such party from a third party that has authority to provide such information or material and without restriction as to disclosure.

15. If a party inadvertently produces "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" material without marking it as such, it may be disclosed to others until the receiving party becomes aware of the error, unless it appears from the face of the document that it contains non-public, confidential, proprietary, commercially sensitive, or trade secret information of the producing party. As soon as the receiving party becomes aware of the inadvertent production, the information must be treated as if it had been timely designated under this Protective Order, and the receiving party must endeavor in good faith to obtain all copies of the material that it distributed or disclosed to persons not authorized to access such information by Paragraphs 5 and 6 above, as well as any copies made by such persons. If timely corrected, an inadvertent failure to designate confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL-ATTORNEYS' EYES ONLY" does not, standing alone, waive the producing party's right to secure protection under this Protective Order for such material.

16. If a party learns that, by inadvertence or otherwise, it has disclosed confidential material to any person or in any circumstance not authorized under this Protective Order, that party must immediately (1) notify in writing the designating party of the unauthorized disclosures, (2) use its best efforts to retrieve all copies of the confidential material, (3) inform the person or persons to whom unauthorized disclosures

were made of all the terms of this Order, and (4) request such person or persons complete and sign a copy of the undertaking in the form attached hereto as Exhibit A.

17. The production of confidential material which are alleged to have been inadvertently produced and are subject to the attorney client privilege, work product immunity or other protection from disclosure, shall not constitute a waiver of such privilege. After receiving notice from the producing party that confidential material subject to protection has been inadvertently produced, the receiving party shall not review, copy or disseminate such confidential material. The receiving party shall return such confidential material to the producing party immediately. Return of the confidential material by the receiving party shall not constitute an admission or concession, or permit any inference, that the returned material is, in fact, properly subject to a claim of attorney-client privilege, work product immunity, or other protection from disclosure, nor shall it foreclose any party from moving the Court for an order that such material has been improperly designated or should be discoverable and/or usable in this litigation for reasons other than a waiver caused by the inadvertent production.

18. It is the present intention of the parties that the provisions of this Protective Order shall govern discovery and other pretrial and trial proceedings in this action. Nonetheless, each of the parties hereto shall be entitled to seek modification of this Protective Order by application to the Court on notice to the other parties hereto for good cause.

19. The provisions of this Protective Order shall, absent written permission of the producing party or further order of the Court, continue to be binding throughout and

after the conclusion of this action, including without limitation any appeals therefrom. Within sixty (60) calendar days after receiving notice of the entry of an order, judgment, or decree finally disposing of this action, including any appeals therefrom, all persons having received confidential material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" hereunder shall return such material and all copies thereof (including summaries and excerpts) to counsel for the producing party, or shall certify destruction thereof. Counsel described in paragraphs 5(a) and 6(a) above shall be entitled to retain court papers, deposition and trial transcripts, and attorney work product (including court papers, transcripts, and attorney work product that contain information or material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY") and to one copy of documents produced by the opposing party designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided that such counsel, and employees of such counsel, shall not disclose any such information and material designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" contained in such court papers, transcripts, attorney work product, or documents to any person or entity except pursuant to a written agreement with the producing party of the information or material. Within 60 days following the expiration of the last period for appeal from any order issued in connection with this action, the parties shall remove any materials designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" from the office of the Clerk of Court. Following that 60-day period, the Clerk of Court shall destroy all designated

"CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" materials.

20. If any party (a) is subpoenaed in another action, (b) is served with a demand in another action to which it is a party, or (c) is served with any other legal process by one not a party to this litigation, seeking information or material which was produced or designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" by someone other than that party, the party shall give prompt actual written notice no more than five (5) court days of receipt of such subpoena, demand, or legal process, to those who produced or designated the confidential material "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" and shall object to its production to the extent permitted by law. Should the person seeking access to the confidential material take action against the party or anyone else covered by this Protective Order to enforce such a subpoena, demand or other legal process, the party shall respond by setting forth the existence of this Protective Order. The designating party shall bear the burdens and the expenses of seeking protection in that court of its confidential material, and nothing in these provisions should be construed as authorizing or encouraging a party in this action to disobey a lawful directive from another court.

21. The parties agree that all designated documents, information, and material exchanged between the parties and subject to this Protective Order in this action shall be used solely for the prosecution or defense of the claims in this action and shall not be

used for any business, commercial, competitive, personal, or other purposes, subject to the other terms of this Protective Order.

22. Nothing in this Protective Order shall prevent outside or inside counsel from giving legal advice based on information that has been designated "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" provided such legal advice shall not reveal the substance of any designated information to a person who is not authorized to receive it.

SO ORDERED, this 24th day of July, 2007

s/ James M. Rosenbaum
JAMES M. ROSENBAUM
United States Chief District Judge

Exhibit A
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)))))))))	Civil Action No. 07-CV-2198 JMR/FLN

STIPULATED PROTECTIVE ORDER

UNDERTAKING OF: _____

1. My home address is:

2. My present employer is and the address of my present employment is:

3. My present occupation or job description is:

4. I have received a copy of the Stipulated Protective Order in this litigation.

5. I have carefully read and understand the provisions of the Stipulated Protective Order in this litigation.

6. I will comply with all of the provisions of the Stipulated Protective Order.

7. I will hold in confidence, will not disclose to anyone not qualified under the Stipulated Protective Order, and will use only for purposes of this litigation, in strict compliance with the terms and conditions of the Stipulated Protective Order, any confidential material which is disclosed to me. I acknowledge that termination of the litigation does not release me from the obligations set out in this paragraph.

8. I will return all confidential information which comes into my possession, and documents or things which I have prepared relating thereto, to counsel for the party

by whom I am employed or retained in strict accordance with the provisions of the Stipulated Protective Order.

9. I hereby submit to the jurisdiction of this Court for the purposes of enforcement of the Stipulated Protective Order in this litigation.

10. Any accompanying resume or curriculum vitae is a complete and accurate statement to the best of my knowledge, and I acknowledge that in submitting such resume or curriculum vitae I know that the receiving party shall rely thereon.

11. I make the above statements under penalty of perjury.

Signature:_____
Date:_____

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.

Defendants.

Case No. 0:07-cv-2198 JMR/FLN

Placeholder For Plaintiff Secure Computing Corporation's Opposition to Defendants' Motion to Dismiss or, in the Alternative, Motion to Transfer Venue

---

This document is a place holder for the following item(s) which are filed in conventional or physical form with the Clerk's Office:

Plaintiff Secure Computing Corporation's Opposition to Defendants' Motion to Dismiss or, in the Alternative, Motion to Transfer Venue [**Filed Under Seal**]

If you are a participant in this case, this filing will be served upon you in conventional format.

This filing was not e-filed for the following reason(s):

____ Voluminous Document* (Document number of order granting leave to file conventionally: _____)

____ Unable to Scan Documents (e.g., PDF file size of one page larger than 2MB, illegible when scanned)

____ Physical Object (description):

____ Non Graphical/Textual Computer File (audio, video, etc.) on CD or other media

_X_ Item Under Seal * [**Document number of protective order: 22**]

____ Item Under Seal pursuant to the Judicial Conference Privacy Policy (General Order 53) (Document number of redacted version: _____)

____ Other (description):

Dated: July 25, 2007

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: s/ Trevor J. Foster

Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (# 313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, Minnesota 55402-2015
(612) 349-8500

ATTORNEYS FOR PLAINTIFF SECURE COMPUTING CORPORATION

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Secure Computing Corp.,

Plaintiff,

v.

Finjan Software Ltd., and
Finjan Software, Inc.

Defendants.

Case No. 0:07-cv-2198 JMR/FLN

LR 7.1(C) Word Count Compliance Certificate Regarding Plaintiff Secure Computing Corporation's Opposition to Defendants' Motion to Dismiss or, in the Alternative, Motion to Transfer Venue

I, Trevor J. Foster, certify that Plaintiff Secure Computing Corporation's Opposition to Defendants' Motion to Dismiss or, in the Alternative, Motion to Transfer Venue complies with Local Rule 7.1(c).

I further certify that, in preparation of this memorandum, I used Microsoft Word, and that this word processing program has been applied specifically to include all text, including headings, footnotes, and quotations in the following word count.

I further certify that the above-referenced memorandum contains 7,419 words.

Dated: July 25, 2007

ROBINS, KAPLAN, MILLER & CIRESI L.L.P.

By: s/Trevor J. Foster
Ronald J. Schutz (#130849)
Jake M. Holdreith (#211011)
Christopher A. Seidl (# 313439)
Trevor J. Foster (#345568)
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
(612) 349-8500

Counsel for Plaintiff
Secure Computing Corporation

SECURE COMPUTING CORPORATION, Plaintiff, v. FINJAN SOFTWARE LTD., and FINJAN SOFTWARE, INC., Defendants.	)	Civil Action No. 07-CV-2198 JMR/FLN

DECLARATION OF PAUL HAWES IN SUPPORT OF PLAINTIFF SECURE COMPUTING CORPORATION'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, MOTION TO TRANSFER VENUE

I, Paul Hawes, declare that:

1. I am currently the Vice President of Human Resources of Secure Computing Corporation ("Secure Computing").

2. Secure Computing is a leading enterprise computer security company that was born out of a division of Honeywell in Minneapolis in 1989. The Company started operations in Roseville, MN.

3. In 1998, Secure Computing moved its headquarters from Roseville, MN to San Jose, CA. The majority of Secure Computing's operations, however, remained in Minnesota.

4. In 2006, Secure Computing's Roseville operations moved to Saint Paul, MN. The Saint Paul facility is approximately 107,000 sq. ft. The majority of Secure Computing's operations, including finance, information technology, manufacturing, order entry, legal, support, and a large portion of research and development, are located in Saint Paul. Approximately 300 employees currently work at the Saint Paul location.

I declare under penalty of perjury that all of the statements made above are true and to the best of my knowledge.

Dated: this 25th, day of July 2007.

Paul Hawes

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation, Plaintiff, v. SECURE COMPUTING CORPORATION, a Delaware corporation; CYBERGUARD CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100, Defendants.	Civil Action No. 06-369-GMS **AFFIDAVIT OF DALE ROSS**

STATE OF MINNESOTA)
) ss.
COUNTY OF RAMSEY)

I, DALE ROSS, being first duly sworn on oath, depose and state that I have personal knowledge of the following facts:

1. My name is Dale Ross. I am over 18 years old. I have worked at Secure Computing Corporation in St. Paul, Minnesota since June 1998. I am currently the Manager of Sales Solutions.

2. On September 22, 2006, I asked a product reseller company, Modcomp, Inc., to purchase Finjan's NG-1100 product. On October 3, 2006, Modcomp provided me a quote for the NG-1100 product. The quote was for an extended price of $22,416.00.

3. On October 12, 2006, Secure Computing provided Modcomp a purchase order for Finjan's NG-1100 for purchase on behalf of Secure Computing Corporation. On October 12,

2006, Secure Computing paid for the NG-1100 order. Secure Computing paid a total of $22,416.00 for the NG-1100 order.

4. On October 24, 2006, Finjan shipped a product that was supposed to be the NG-1100 from San Jose, California directly to Secure Computing in St. Paul, Minnesota. Secure Computing received the shipment in St. Paul, Minnesota on October 31, 2006. However, the product's shipping boxes and the actual product was labeled Vital Security Internet 1Box™.

5. On about April 10, 2007, I asked Modcomp to purchase Finjan's Load Balancer product. On April 13, 2007, Modcomp provided me a quote for the Load Balancer order. The quote was for an extended price of $7,900.00.

6. On April 19, 2007, Secure Computing provided Modcomp a purchase order for Finjan's Load Balancer product for purchase on behalf of Secure Computing Corporation. On April 19, 2007, Secure Computing paid for the Load Balancer order. Secure Computing paid a total of $7,900.00 for the Load Balancer order.

7. On April 26, 2007, Finjan's Load Balancer product was delivered and arrived from Finjan in San Jose, California directly to Minnesota.

FURTHER, AFFIANT SAYETH NOT.

Dated: May 15, 2007

Dale Ross

Subscribed and sworn to before me
this 15th day of May, 2007.

MARY K BUDGE
Notary Public
Minnesota
My Commission Expires January 31, 2010

Notary Public