Peter R. Afrasiabi (Bar No. 193336)
Christopher W. Arledge (Bar No. 200767)
TURNER GREEN AFRASIABI & ARLEDGE LLP
535 Anton Boulevard, Suite 850
Costa Mesa, California 92626
Telephone: (714) 434-8750
Facsimile: (714) 434-8756

Attorneys for Plaintiff Network Signatures, Inc.

FILED
2009 MAR 26 PM 3:46
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
SANTA ANA
BY

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

**SOUTHERN DIVISION**

Network Signatures, Inc.,

Plaintiff,

v.

Fidelity Investments Institutional Services Company, Inc., a Massachusetts corporation,

Defendant.

Case No. **SACV09 -376 MRP (FMOx)**

**COMPLAINT FOR PATENT INFRINGEMENT, PERMANENT INJUNCTION AND DAMAGES**

**DEMAND FOR JURY TRIAL**

For its Complaint against Defendant Fidelity Investments Institutional Services Company, Inc. ("Defendant"), Plaintiff Network Signatures, Inc. ("Network Signatures") alleges as follows:

## THE NAVAL RESEARCH LABORATORY

1. The Naval Research Laboratory ("NRL") is one of the most accomplished research-and-development organizations in the country. NRL scientists have not only made remarkable breakthroughs in military technology, they have literally changed the world for all of us. Without their efforts, we would not have GPS, modern radar, and any number of other technological innovations that we now take for granted. This lawsuit concerns another such innovation: technology that allows for the safe and secure communication of sensitive information via the Internet, such as personal, banking, commercial, financial, and other information.

2. Federal law empowers the government to license its patents to private parties for commercialization as well as for enforcement of the patent without the United States as a party. 37 C.F.R. § 404.5(b)(2). By doing so, the government can use market forces to better capitalize on its technologies the way a private party would. In addition, a license agreement can give the private licensee the proper incentives to protect the government's intellectual property from theft, a task often handled better by a private entity.

## THE PARTIES

3. Plaintiff Network Signatures, Inc. ("Network Signatures") is a corporation duly organized and existing under the laws of Delaware with its principal place of business 30021 Tomas Street, Suite 300, Rancho Santa Margarita, California 92688. As alleged below, the United States of America has granted to Network Signatures an exclusive license concerning the patented technology at issue in this lawsuit.

4. Defendant is a corporation duly organized and existing under the laws of the State of Massachusetts, with its principal place of business at Fidelity Investments Institutional Services Company, Inc., 82 Devonshire St., Boston, MA 02109. Defendant is in the business of providing financial products and services to persons in the U.S. and worldwide through physical and electronic channels, including the Internet.

## JURISDICTION AND VENUE

5. This is a civil action for patent infringement arising under the Patent Act of the United States, 35 U.S.C. §§ 1 et seq. This court has subject matter jurisdiction of such federal question claims pursuant to 28 U.S.C. §§ 1331 and 1338(a).

6. Venue is proper under 28 U.S.C. §§ 1391(b), 1391(c) and 1400(b) in that the acts and transactions complained of herein were conceived, carried out, made effective, and had effect within the State of California and within this district, among other places. Defendant resides in this judicial district by virtue of its business activities in this district, have committed acts of infringement in this judicial district, or have committed acts of contributory infringement and inducement of infringement within this judicial district.

## NETWORK SIGNATURES LICENSES THE NAVY'S TECHNOLOGY

7. On April 23, 1996, the United States Patent & Trademark Office duly and legally issued United States Letters Patent No. 5,511,122 ("the '122 Patent"), entitled "Intermediate Network Authentication."

8. The '122 patent claims, among other things, a critical method of authenticating a computer in which a private electronic key is used, together with a validating public electronic key, to create a cryptographic signature, the cryptographic signature is transmitted in at least one packet to the validating computer, and the signature is verified by the validating computer using its private key and the public key of the computer to be authenticated. This authentication method allows for the safe and secure communication of sensitive information, such as personal, banking, commercial, financial, and other information, as is transmitted between computers by Defendant and its customers and users herein.

9. The '122 Patent is owned by the United States of America, as represented by the Secretary of the Navy. To allow enforcement, commercialization of and protection of this patent and the technology it represents, in September 2004, the United States Navy executed an exclusive license agreement with Metrix Services, Inc. ("Exclusive License Agreement") and, by this Exclusive License Agreement, expressly granted Metrix Services the exclusive right to practice, enforce, and sublicense, among other rights, the '122 Patent, subject to the general limitations imposed by federal law. A true and correct copy of the Exclusive License Agreement is attached hereto as Exhibit A and incorporated herein by reference. With the express approval of the United States Navy, Metrix Services transferred its entire right, title, and interest to, and in, the '122 Patent to Network Signatures on February 14, 2006. A true and correct copy of the First Amendment to the Exclusive License Agreement, which, among other things, approved the assignment of the Exclusive License Agreement to Network Signatures, is attached hereto as Exhibit B and incorporated herein by reference. A true and correct copy of the Assignment from Metrix to Network Signatures is attached as Exhibit C and incorporated herein by reference.

10. Pursuant to its rights under the Exclusive License Agreement, Network Signatures has begun the commercial development of a product, known as EasyConnect, that utilizes the '122 Patent. Network Signatures has demonstrated the product to NRL personnel and has received NRL's recognition of its development efforts. A true and correct copy of an October 12, 2006, letter from the Navy to Network Signatures reflects this and is attached as Exhibit D and incorporated by reference herein.

11. Network Signatures has also begun exercising its other primary obligation under the Exclusive License Agreement: protecting the Navy's intellectual property rights from infringement.

**FIRST CLAIM FOR RELIEF**

**AGAINST DEFENDANT FOR DIRECT, CONTRIBUTORY AND INDUCING INFRINGEMENT OF U.S. PATENT NO. 5,511,122**

12. Plaintiff incorporates herein by reference the allegations set forth in paragraphs 1-11 of the Complaint as though fully set forth herein.

13. A true and correct copy of the '122 Patent is attached as Exhibit E and incorporated herein by reference. On information and belief, Defendant uses digital certificates and digital signatures implemented though the use of public key infrastructure to facilitate communication with its employees and customers. For example, Defendant enables a computer of a Defendant customer, affiliate, business partner, or employee ("sending computer") to send a secure communication over the Internet to another computer ("receiving computer") by using a confidential private key, and a public key, to digitally sign the message being sent. When the receiving computer receives the signed message, it uses the sending computer's public key, and its private key, to decrypt the signature (collectively referred to as "Defendant Authentication Activities").

14. By making, using, selling, and offering for sale Defendant Authentication Activities, Defendant has directly infringed and continues to directly infringe the '122 Patent, including infringement under 35 U.S.C. § 271(a) and (f).

15. On information and belief, Defendant has also indirectly infringed and continues to indirectly infringe the '122 Patent by actively inducing direct infringement by other persons—specifically, customers and partners of Defendant—who operate methods that embody or otherwise practice one or more of the claims of the '122 Patent when Defendant had knowledge of the '122 Patent and knew or should have known that their actions would induce direct infringement by others and intended that their actions would induce direct infringement by others.

16. On information and belief, Defendant has also indirectly infringed and continues to indirectly infringe the '122 Patent by contributory infringement by providing non-staple articles of commerce to others for use in an infringing system or method with knowledge of the '122 Patent and knowledge that these non-staple articles of commerce are used as a material part of the claimed invention of the '122 Patent.

17. On information and belief, Defendant's foregoing acts of infringement include infringement by use and implementation of the Defendant Authentication Activities which are made part of their financial products and services.

18. On information and belief, Defendant will continue to infringe the '122 Patent unless enjoined by this Court.

19. On information and belief, Defendant's infringement of the '122 Patent is, has been, and continues to be willful and deliberate.

20. As a direct and proximate result of Defendant's infringement of the '122 Patent, Network Signatures and the United States Government have been and continue to be damaged in an amount yet to be determined.

21. Unless a preliminary and permanent injunction are issued enjoining Defendant and its officers, agents, servants and employees, and all others acting on their behalf or in concert with Defendant, from infringing the '122 Patent, Network Signatures, and the United States Government, will be greatly and irreparably harmed.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff Network Signatures prays for judgment against Defendant as follows:

(1) For a judicial determination and declaration that Defendant has directly infringed, and continues to directly infringe, United States Letters Patent No. 5,511,122;

(2) For a judicial determination and declaration that Defendant has induced, and continues to induce, the infringement of United States Letters Patent No. 5,511,122;

(3) For a judicial determination and declaration that Defendant has contributorily infringed, and continues to contributorily infringe, United States Letters Patent No. 5,511,122;

(4) For a judicial determination and decree that Defendant's infringement of United States Letters Patent No. 5,511,122 has been, and continues to be, willful and deliberate;

(5) For a judicial determination and decree that Defendant, its respective subsidiaries, officers, agents, servants, employees, licensees, and all other persons or entities acting or attempting to act in active concert or participation with it or acting on its behalf, be preliminarily and permanently enjoined from further infringement of the '122 Patent;

(6) For a declaration that Defendant notify all of its customers and users of the infringing system and customers' participation in the infringement with Defendant's encouragement, and that Defendant encourage customers to cease all such infringing actions;

(7) For a judicial decree that orders Defendant to account for and pay to Network Signatures all damages caused to Network Signatures by reason of Defendant's infringement pursuant to 35 U.S.C. Section 284, including enhanced damages under 35 U.S.C. Section 285;

(8) For an award of damages according to proof at trial;

(9) For a judicial declaration that this case is exceptional under 35 U.S.C. Section 285 and Defendant be ordered to pay Network Signatures' costs, expenses, and reasonable attorney's fees pursuant to 35 U.S.C. Sections 284 and 285;

(10) For a judicial order awarding to Network Signatures pre-judgment and post-judgment interest on the damages caused to it by Defendant's infringement; and

(11) For any such other and further relief as the Court may deem just and proper under the circumstances.

Dated: March 24, 2009

**TURNER GREEN AFRASIABI & ARLEDGE LLP**

By: _____
Peter R. Afrasiabi
Attorneys for Plaintiff, Network Signatures, Inc.

**DEMAND FOR JURY TRIAL**

Plaintiff Network Signatures, Inc. hereby demands trial by jury in this action.

Dated: March 24, 2009

**TURNER GREEN AFRASIABI & ARLEDGE LLP**

By: _____

Peter R. Afrasiabi

Attorneys for Plaintiff, Network Signatures, Inc.

27 September 2004

EXCLUSIVE LICENSE

Between

METRIX SERVICES, INC.

And

UNITED STATES OF AMERICA

As Represented By

THE SECRETARY OF THE NAVY

NRL-LIC-04-23-161

EXHIBIT A

(3)

27 September 2007

INDEX


| | | Page |
|---|---|---|
| Preamble | | 3 |
| Article I | Definitions | 6 |
| Article II | LICENSE Grant | 8 |
| Article III | LICENSEE's Performance | 9 |
| Article IV | Royalties | 10 |
| Article V | Patent Marking and Nonendorsement | 13 |
| Article VI | Representation and Warranties | 13 |
| Article VII | Reports | 14 |
| Article VIII | Modification and Termination | 15 |
| Article IX | Notice | 17 |
| Article X | Sublicensing | 18 |
| Article XI | Reservation of Rights | 19 |
| Article XII | Litigation | 20 |




(4)

27 September 2004

PREAMBLE

This exclusive license (hereinafter called "LICENSE") is made and entered into by and between the United States of America as represented by the Secretary of the Navy (hereinafter called "LICENSOR") and Metrix Services, Inc., a corporation organized and existing under the laws of the State of California (hereinafter called "LICENSEE") having an address at 2 Peters Canyon, Irvine, CA 92606.

WITNESSETH:

WHEREAS Title 35 of the United States Code, Section 207, authorizes Federal agencies to license their patents; and

WHEREAS Title 37 of the Code of Federal Regulations, Chapter IV, Part 404 entitled "Licensing of Government Owned Inventions" sets forth the terms and conditions under which licenses may be granted; and

WHEREAS the above-cited authorities provide that licensing of Government inventions will best serve the interests of the Federal Government and the public when utilization of such inventions is promoted and such inventions are brought to Practical Application; and

WHEREAS LICENSOR has an assignment of full right, title, and interest to the invention disclosed and claimed in U.S. Patent No. 5,511,122 issued on April 23, 1996, for "Intermediate Network Authentication"; and



5

27 September 2004

WHEREAS LICENSOR has published in the Federal Register of December 17, 1996, the availability of a license under U.S. Patent No. 5,511,122; and

WHEREAS LICENSEE has supplied LICENSOR with a plan for development and marketing of this invention and has expressed its intention to carry out this plan upon the granting of this LICENSE; and

WHEREAS LICENSEE has agreed that any products embodying this invention or produced through the use of this invention for use or sale in the United States will be manufactured substantially in the United States; and

WHEREAS LICENSOR has published in the Federal Register of September 9, 2004, notice of its intention to grant this LICENSE under U.S. Patent No. 5,511,122 to LICENSEE and has provided the public with an opportunity for filing written objections; and

WHEREAS LICENSOR has determined that:

(A) The interest of the Federal Government and the public will best be served by the proposed license, in view of the LICENSEE's intentions, plans, and ability to bring the invention described and claimed in U.S. Patent No. 5,511,122 to Practical Application or otherwise promote the invention's utilisation by the public;

(B) The desired Practical Application has not been achieved, or is not likely expeditiously to be achieved, under any

nonexclusive license which has been granted, or which may be granted, on the invention;

(C) Exclusive licensing is a reasonable and necessary incentive to call forth the investment of risk capital and expenditures to bring the invention to Practical Application or otherwise promote the invention's utilization by the public;

(D) The proposed terms and scope of exclusivity are not greater than reasonably necessary to provide the incentive for bringing the invention to Practical Application or otherwise promote the invention's utilization by the public; and

WHEREAS LICENSOR has not determined that the grant of this LICENSE will tend substantially to lessen competition or result in undue concentration in any section of the country in any line of commerce to which the technology to be licensed relates or to create or maintain other situations inconsistent with the antitrust laws; and

WHEREAS LICENSOR has considered the capabilities of LICENSEE to bring the invention to Practical Application and has found that the LICENSEE is a responsible party for negotiating this LICENSE on terms and conditions most favorable to the public interest and that to grant this exclusive LICENSE would be in the public interest;

NOW, therefore, in accordance with and to the extent provided by the aforementioned authorities and in consideration of the foregoing premises and of the covenants and obligations



(7)

hereinafter set forth to be well and truly performed, and other good and valuable consideration, the parties hereto agree to the foregoing and as follows:

ARTICLE I

Definitions

The following definitions shall apply to the defined words where such words are used in this LICENSE:

A. The "Licensed Patent" means U.S. Patent No. 5,511,122 entitled "Intermediate Network Authentication" issued April 23, 1996, to Randall Atkinson;

B. A "Licensed Invention" means an invention claimed in the Licensed Patent and any patents issuing thereon;

C. To "Practice the Licensed Invention" means to make, use, import, offer for sale, and sell by or on behalf of LICENSEE or otherwise dispose of according to law any machine, article of manufacture, composition of matter, or process physically embodying or made according to a Licensed Invention;

D. "Practical Application" means to manufacture in the case of a composition, product or article of manufacture, to practice in the case of a process or method, or to operate in the case of a machine or system, and, in each case under such conditions as to establish that a Licensed Invention is being utilized and that its benefits are to the extent permitted by law and Government regulations available to the public on reasonable terms;



(6)

27 September 2004

E. A "Royalty-Bearing Product" means any product defined by any claim of the Licensed Patent or made by a method claimed in the Licensed Patent;

F. "Net Selling Price" shall mean the invoice price of the Royalty-Bearing Product sold less all discounts and rebates actually allowed, allowances actually granted on account of rejections, returns, or billing errors, and separately billed duties, insurance, taxes, and other government or regulatory charges. A Royalty-Bearing Product will be considered to be sold when shipped or delivered to a customer or, in case of a service, will be considered to be sold when placed into service for a customer or made available to a customer for use.

G. "United States" means the United States of America, its territories and possessions, the District of Columbia, and the Commonwealth of Puerto Rico;

H. A "Grace Period" is the period after September 30 of a calendar year and before January 1 of the following calendar year; and

I. "AFFILIATE" shall mean any company, corporation, association or business in which LICENSEE owns directly or indirectly a controlling interest.

J. "SUBLICENSEE" shall mean any non-AFFILIATE granted a sublicense under Article X;



(9)

27 September 2004

K. "Sublicense Income" shall mean any payments that LICENSEE or an AFFILIATE receives from a SUBLICENSEE in consideration of the sublicense of the rights granted by LICENSEE and AFFILIATES under Article K, including without limitation license fees, milestone payments, license maintenance fees, royalty fees, upfront fees, one-time royalties and other payments.

## ARTICLE II

## LICENSE Grant

LICENSOR grants to LICENSEE an exclusive right and license to Practice the Licensed Invention throughout the United States commencing on the date of execution of this LICENSE by LICENSOR, which shall become the effective date of the LICENSE, until the expiration of U.S. Patent No. 5,511,122 unless the LICENSE is sooner modified or terminated in whole or in part.

LICENSOR hereby grants to LICENSEE the right to extend the LICENSE granted hereunder to one or more AFFILIATES subject to the terms and conditions hereof, provided that the AFFILIATE is not directly or indirectly controlled by a foreign company, corporation, association, business or government.

This LICENSE is nonassignable without written approval of LICENSOR except to the successor of that part of LICENSEE's business to which this Licensed Invention pertains, provided that the successor is not directly or indirectly controlled by a foreign company, corporation, association, business or government.

27 September 2004

ARTICLE III

LICENSEE's Performance

LICENSEE agrees to carry out the plan for development and marketing of a Licensed Invention submitted with LICENSEE's Application for License dated August 27, 2004 and amended September 13, 2004, to bring this Licensed Invention to Practical Application one (1) year from date of execution of the LICENSE and LICENSEE will, thereafter, continue to make the benefits of this Licensed Invention reasonably accessible to the public for the remainder of the period of this LICENSE.

LICENSEE agrees that during the period of this LICENSE any products embodying this Licensed Invention or produced through the use of a Licensed Invention for use or sale by LICENSEE or its sublicensees in the United States will be manufactured substantially in the United States.

LICENSEE shall pay to the LICENSOR a non-refundable licensing fee in the amount of twenty five hundred dollars ($2,500) payable upon the execution of this LICENSE by LICENSEE. Payment will be made in the manner prescribed in Article IV.

LICENSEE agrees to promptly report to LICENSOR any changes in mailing address, name or company affiliation during the period of this LICENSE and to promptly report discontinuance of LICENSEE's making the benefits of this Licensed Invention reasonably accessible to the United States public.



(1)

27 September 2004

ARTICLE IV

Royalties

LICENSEE shall pay a royalty to LICENSOR of three percent (3%) of the Net Selling Price for each Royalty-Bearing Product made, used, or sold by LICENSEE or its licensed AFFILIATES. LICENSEE shall also pay a royalty to LICENSOR of three percent (3%) of the Sublicensee Income. Notwithstanding the above, in no event shall any single sale or license be subjected to the payment of a royalty greater than 3% or multiple royalties of 3%.

If a Royalty-Bearing Product is distributed in whole or in part for non-cash consideration (whether or not at a discount), the Net Selling Price shall be calculated as the price of the Royalty-Bearing Product charged to an independent third party during the same royalty reporting period, or in the absence of such sales, on the fair market value of the Royalty-Bearing Product.

Non-cash consideration shall not be accepted by LICENSEE or any sublicensee for the sale of any Royalty-Bearing Product without the prior written consent of LICENSOR.

Royalties will not be paid on items sold directly to agencies of the U.S. Government or for known U.S. Government end use.

On sales made between LICENSEE and its AFFILIATES or sublicensees for resale, the royalty shall be paid on the higher Net Selling Price.

27 September 2004

Notwithstanding the provisions of the preceding paragraphs in this Article IV, LICENSEE agrees to pay at least a minimum annual royalty of ten thousand dollars ($10,000) for calendar year 2006, and each calendar year thereafter throughout the period of the LICENSE. The minimum annual royalty for each calendar year shall be due and payable in advance on or before September 30 of the preceding year and will be credited as advance payment of royalties to accrue during the calendar year following payment. The minimum annual royalty payments will not be refunded in whole or in part.

LICENSEE shall send to LICENSOR all royalties which accrue between January 1 and December 31 of each year by February 28 of the following year. A royalty report shall be included with each payment setting forth the quantity and Net Selling Price of each Royalty-Bearing Product sold during the period covered by the report, to whom sold and the date of such sale, and the total amount of royalties being paid for that year. Royalty reports are due each calendar year. The last royalty report is due sixty (60) days after the expiration of this LICENSE.

All payments due LICENSOR under this LICENSE shall be paid in United States dollar amounts to the DFAS-CH DSSN 8347 and mailed to:

Office of Naval Research
Patent Counsel of the Navy (ONR 01CC)
800 N. Quincy Street
Arlington, VA 22217-5660



13

with a copy of each royalty report to:

Head, Technology Transfer Office
Naval Research Laboratory, Code 1004
4555 Overlook Ave., SW
Washington, DC 20375-5320

LICENSEE agrees to make and keep and shall require its AFFILIATES and sublicensees to make and keep full, accurate and complete books and records (together with supporting documentation) as are necessary to establish its compliance with this Article IV. Such records shall be retained for at least three (3) years following the end of the reporting period to which they relate.

LICENSEE agrees that LICENSOR may, if LICENSOR so desires at a future time or times, have a duly authorized agent or representative in LICENSOR's behalf examine all such books and records and supporting documentation either at LICENSEE's business premises or at a place mutually agreed upon by LICENSEE and LICENSOR for the sole purpose of verifying reports and payments hereunder. In conducting examinations pursuant to this paragraph, LICENSOR's representative shall have access to all records that LICENSOR reasonably believes to be relevant to the calculation of royalties under Article IV. If a royalty payment deficiency is determined, LICENSEE shall pay the royalty deficiency outstanding within thirty (30) days of receiving written notice thereof. Payments made by LICENSEE after the due date shall include interest at the annual rate of two percentage points above the



(14)

27 September 2004

Prime Rate (as reported in the Wall Street Journal for the due date) for the period of lateness. Such examination by LICENSOR's representative shall be at LICENSOR's expense, except that if such examination shows an underreporting or underpayment in excess of five percent (5%) for any twelve (12) month period, then LICENSEE shall pay the cost of such examination.

ARTICLE V

Patent Marking and Nonendorsement

LICENSEE hereby agrees to mark each product manufactured or sold under this LICENSE (or when the character of the product precludes marking, the package containing any such product) with the notation "Licensed from U.S. Navy under U.S. Patent No. 5,511,122". LICENSEE agrees not to create the appearance that LICENSOR endorses LICENSEE's business or products.

ARTICLE VI

Representation and Warranties

LICENSOR makes no representation or warranty as to validity of U.S. Patent No. 5,511,122 or of the scope of any of the claims contained therein or that the exercise of this LICENSE will not result in the infringement of other patent(s). Neither LICENSOR nor its employees assumes any liability whatsoever resulting from the exercise of this LICENSE.

Nothing relating to the grant of this LICENSE, nor the grant itself, shall be construed to confer upon LICENSEE or any sub-licensee hereunder or any other person any immunity from or defenses under the antitrust laws or from a charge of patent misuse, and the acquisition and use of rights pursuant to this LICENSE shall not be immunized from the operation of State or Federal law by reason of the source of the grant.

Nothing contained in this LICENSE shall be interpreted to grant to LICENSEE any rights with respect to any invention other than the Licensed Invention.

ARTICLE VII

Reports

LICENSEE agrees to submit annual reports on or before March 1 of each calendar year on its efforts to achieve Practical Application of the Licensed Invention by one (1) year from date of execution of the LICENSE, with particular reference to LICENSEE's plan for development and marketing of the Licensed Invention submitted with LICENSEE's application for license. These reports shall contain a discussion of the actual number of staff and dollars spent during the preceding year committed to the commercialization effort. These reports shall contain information within LICENSEE's knowledge, or which it may acquire under normal business practices, pertaining to the commercial use being made of this Licensed Invention and other information which LICENSOR may

determine is pertinent to Government licensing activities. LICENSEE agrees to submit such reports to LICENSOR until such time that the invention has been brought to the point of Practical Application.

ARTICLE VIII

Modification and Termination

This LICENSE may be terminated in whole or in part by LICENSOR if:

(A) LICENSOR determines that LICENSEE is not executing the plan submitted with the request for license dated August 27, 2004 and amended September 13, 2004, and LICENSEE cannot otherwise demonstrate to the satisfaction of LICENSOR that it has taken or can be expected to take within a reasonable time effective steps to achieve Practical Application of this Licensed Invention;

(B) LICENSOR determines that such action is necessary to meet requirements for public use specified by Federal regulations issued after the date of this LICENSE and such requirements are not reasonably satisfied by LICENSEE;

(C) LICENSEE willfully made a false statement of or willfully omitted a material fact in its application for license or in any report required by this LICENSE; or

(D) LICENSEE commits a substantial breach of a covenant or agreement herein contained.



(17)

27 September 2004

LICENSEE may terminate this LICENSE by providing a written notice of termination to LICENSOR. LICENSEE's written notice must include LICENSEE's statement that neither the LICENSEE nor its sublicensees nor any LICENSE AFFILIATES will practice the Licensed Invention in the United States after the LICENSE terminates. LICENSEE's written notice shall specify the effective date of termination.

This LICENSE may be modified or terminated in whole or in part consistent with the law and applicable regulations upon mutual agreement of LICENSOR and LICENSEE evidenced in writing and signed by both parties.

This LICENSE may be restricted to the fields of use or geographic areas, or both, in which the LICENSEE has brought the invention to Practical Application and continues to make the benefits of the invention reasonably accessible to the public. However, such restriction may be made only after the expiration of seven (7) years following the effective date of this LICENSE.

LICENSEE may request modification of this LICENSE in writing sent to LICENSOR and stating the reasons therefor.

Before modifying or terminating in whole or in part this LICENSE for any cause other than by mutual agreement, LICENSOR shall furnish LICENSEE and each sublicensee of record a written notice of intention to modify or terminate in whole or in part this LICENSE, and LICENSEE and any sublicensee shall be allowed thirty (30) days after such notice or other agreed-upon time

period, whichever is greater, to remedy any breach of any covenant or agreement set forth in this LICENSE or to show cause why this LICENSE should not be modified or terminated in whole or in part.

LICENSEE has a right to appeal, in accordance with procedures prescribed by the Chief of Naval Research, any decision or determination concerning the interpretation, modification, termination in whole or in part of this LICENSE.

Notwithstanding the provisions of Article II, LICENSEE and LICENSOR agree that this LICENSE shall automatically terminate on September 30 of any year if the minimum annual royalty due for the following calendar year, as expressed in Article IV of this LICENSE, is not timely paid. If, however, the minimum annual royalty payment together with a surcharge of one hundred fifty dollars ($150) is paid during the Grace Period before the following calendar year, then this LICENSE shall be considered as not having automatically terminated.

ARTICLE IX

Notice

All communications and notices required under this LICENSE shall be considered duly given if sent by courier requiring signed receipt upon delivery or if timely mailed by U.S. Postal Service, first class, postage prepaid and addressed as follows:

27 September 2004

(a) if to LICENSOR:

Office of Naval Research
Patent Counsel of the Navy (ONR 01CC)
800 N. Quincy Street
Arlington, VA 22217-5660

with a copy to:

Head, Technology Transfer Office
Naval Research Laboratory, Code 1004
4555 Overlook Ave., SW
Washington, DC 20375-5320

(b) if to LICENSEE:

Hazim Ansari
Metrix Services, Inc.
2 Peters Canyon
Irvine, CA 92606

or such mailing address as either party may from time to time specify in writing.

ARTICLE X

Sublicensing

LICENSEE may grant, subject to the approval of LICENSOR, sublicenses under this LICENSE upon terms and conditions that LICENSEE may arrange provided that:

A. Each sublicense shall be in writing and make reference to this LICENSE including the rights retained by LICENSOR under this LICENSE; and

B. Each sublicense shall specify that it is granted pursuant to this LICENSE, shall specify that no provision shall be in derogation of or diminish any rights in this LICENSE and shall include the condition that the sublicense shall automatically be



20

modified or terminated in whole or in part upon the modification or termination in whole or in part of this LICENSE; and

C. LICENSEE shall furnish LICENSOR with a copy of the standard sublicense agreement for approval thirty (30) days before the first sublicense is granted. When substantial changes are made to the standard sublicense agreement, LICENSEE shall provide LICENSOR a copy of the modified sublicensee for approval thirty (30) days before LICENSEE shall grant any sublicense thereunder.

D. The granting of any sublicense by LICENSEE shall in no way relieve LICENSEE from any of the requirements of this LICENSE including royalties. Any sublicense granted by LICENSEE that does not comply with the requirements of this Article X is void.

## ARTICLE XI

## Reservation of Rights

LICENSOR reserves the right to require LICENSEE to and LICENSEE agrees to grant promptly sublicenses to responsible applicants on reasonable terms when necessary to fulfill health and safety needs of the public to the extent such needs are not being reasonably satisfied by LICENSEE and its sublicensees.

This LICENSE is subject to the irrevocable, royalty-free right of the Government of the United States to practice and have practiced this Licensed Invention throughout the world by or on behalf of the United States and by or on behalf of any foreign government or intergovernmental or international organization

pursuant to any existing or future treaty or agreement with the Government of the United States.

This LICENSE is subject to any licenses in force at the time of the grant of this LICENSE.

ARTICLE XII

Litigation

LICENSOR does not by entering into this LICENSE transfer the property rights in the Licensed Invention, provided however, that during the period that this LICENSE is exclusive, LICENSEE has the right of enforcement of the Licensed Patent, at no cost to the Government and without requiring the Government to be a party to the litigation, pursuant to the provisions of Chapter 29 of Title 35, United States Code, or other statutes. LICENSEE shall pay LICENSOR thirty percent (30%) of the actual recovery after deduction of LICENSEE's litigation costs and expenses.

IN WITNESS WHEREOF, the parties hereto have caused this instrument to be executed by their duly authorized representatives.

UNITED STATES OF AMERICA
For the Secretary of the Navy

By: _____
D.M. SCHUBERT
Captain, U.S. Navy
Commanding Officer

Date: 9/25/04

METRIX SERVICES, INC.

By: _____
HAKIM ANSARI

Title: CEO

Date: 9/28/04

# FIRST AMENDMENT TO EXCLUSIVE LICENSE AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AS REPRESENTED BY THE SECRETARY OF THE NAVY AND METRIX SERVICES, INC.

The Exclusive License Agreement executed on September 28, 2004, (hereinafter called "LICENSE") between the United States of America, as represented by the Secretary of the Navy, (hereinafter called "LICENSOR"), and Metrix Services, Inc., a corporation organized and existing under the laws of the State of California, (hereinafter called "LICENSEE") having an address at 2 Peters Canyon, Irvine, CA 92606 is hereby amended by mutual agreement.

WHEREAS, LICENSOR desires the grant of sublicensing rights to LICENSEE be clarified; and

WHEREAS, LICENSEE desires the LICENSE be assigned to their successor in part Network Signatures, LLC; and

WHEREAS, LICENSEE desires the removal of the requirement that products be manufactured substantially in the United States; and

WHEREAS, LICENSEE desires the Practical Application date be extended; and

WHEREAS, LICENSEE desires the litigation clause be clarified to include the right of the LICENSEE to collect for past and future infringement; and

WHEREAS, LICENSOR desires the litigation clause be modified to require LICENSEE obtain LICENSOR's approval before enforcing the Licensed Patent;

NOW, WHEREFORE, LICENSOR and LICENSEE agree to amend the LICENSE as follows:

1. The LICENSE shall be assigned to Network Signatures, LLC.

2. Article III, paragraph 1 shall now read:

LICENSEE agrees to carry out the plan for development and marketing of a Licensed Invention submitted with LICENSEE's Application for License dated August 27, 2004 and amended September 13, 2004, to bring this Licensed Invention to Practical Application two (2) years from date of execution of the LICENSE and LICENSEE will, thereafter, continue to make the benefits of this Licensed Invention reasonably accessible to the public for the remainder of the period of this LICENSE.

3. Article III, paragraph 2 shall now read:

LICENSOR agrees that products embodying this Licensed Invention or produced through the use of a Licensed Invention for use or sale by LICENSEE, its AFFILIATES or its sublicensees in the United States do not need to be manufactured substantially in the United States. Notwithstanding the above, products embodying this Licensed Invention or produced through the use of a Licensed Invention for use or sale by LICENSEE, its AFFILIATES or its sublicensees cannot be manufactured in any of the countries identified: (1) in the Treasury Department Office of Foreign Assets Control schedule in 31 C.F.R. § 500.201; (2) in the State Department Directorate of Defense Trade Controls list in 22 C.F.R. § 126.1(a); or (3) on the Treasury Department Office of Foreign Assets Control website for sanctioned countries (http://www.treas.gov/offices/enforcement/ofac/sanctions/).

4. Article IV, paragraph 1 shall now read:

LICENSEE shall pay a royalty to LICENSOR of three percent (3%) of the Net Selling Price for each Royalty-Bearing Product made, used, or sold by LICENSEE and its licensed AFFILIATES. LICENSEE shall pay LICENSOR thirty percent (30%) of any consideration received from a SUBLICENSEE for a sublicense except in the case of litigation where LICENSEE shall pay LICENSOR thirty percent (30%) of the actual recovery after deduction of LICENSEE's litigation costs and expenses as provided in Article XII.

5. Article VII, sentence 1 shall now read:

LICENSEE agrees to submit annual reports on or before March 1 of each calendar year on its efforts to achieve Practical Application of the Licensed Invention by two (2) years from date of execution of the LICENSE, with particular reference to LICENSEE's plan for development and marketing of the Licensed Invention submitted with LICENSEE's application for license.

6. Payments and reports required under Article IV and communications and notices required under Article XI shall now be sent to:

(a) if to LICENSOR:

Office of Naval Research
Office of Corporate Counsel (ONR BDCC)
One Liberty Center
875 North Randolph Street
Arlington, VA 22203-1995

with a copy to:

Head, Technology Transfer Office
Naval Research Laboratory, Code 1004
4555 Overlook Ave., SW
Washington, DC 20375-5320

(b) if to LICENSEE:

Hazim Ansari
Network Signatures, LLC
14252 Culver Dr., 914
Irvine, CA 92604

7. Article XII shall now read:

LICENSOR does not by entering into this LICENSE transfer the property rights in the Licensed Invention, provided however, that during the period that this LICENSE is exclusive, LICENSEE has the right of enforcement of the Licensed Patent, at no cost to the Government and without requiring the Government to be a party to the litigation, pursuant to the provisions of Chapter 29 of Title 35, United States Code, or other statutes. LICENSEE shall inform LICENSOR of any action, legal or otherwise, it intends to take with respect to the rights prior to taking such action. LICENSOR has the right to object to such action within ten (10) days of receiving notification of such action. If LICENSOR does not respond within the ten (10) day period, LICENSOR shall be deemed to not object to the proposed action. LICENSEE's right of enforcement expressly includes the right to collect damages for past and future infringement of the Licensed Patent to the extent permissible under law. LICENSEE shall pay LICENSOR thirty percent (30%) of the actual recovery after deduction of LICENSEE's litigation costs and expenses.

IN WITNESS WHEREOF, the parties hereto have caused this instrument to be executed by their duly authorized representatives.

UNITED STATES OF AMERICA
For the Secretary of the Navy

By: _____
D.R. GAHAGAN
Captain, U.S. Navy
Commanding Officer

Date: 6 FEB 06

METRIX SERVICES, INC.

By: _____
HAZIM ANSARI
Title: CEO

Date: 2/14/06

NETWORK SIGNATURES, LLC

By: _____

Date: 2/14/06

# ASSIGNMENT

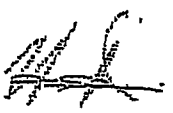
WHEREAS, Metrix Services, Inc. having a principal place of business in Tustin, California, owns an Exclusive License to U.S. Patent No. 5,511,122, entitled "Intermediate Network Authentication" and has been granted such Exclusive License from the United States of America, as represented by the Secretary of the Navy. (hereinafter "Exclusive License");

AND WHEREAS, Network Signatures (hereinafter "ASSIGNEE"), with its principal place of business in Vista, California, desires to acquire the entire right, title, and interest in and to the said Exclusive License:

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt of which is hereby acknowledged, Metrix Services does hereby acknowledge that it has sold, assigned, transferred and set over, and by these presents do hereby sell, assign, transfer and set over, unto the said ASSIGNEE, its successors, legal representatives and assigns, the entire right, title, and interest throughout the world in, to and under the said improvements, and the said Exclusive License and all provisional applications relating thereto, and all divisions, renewals and continuations or continuations-in-part thereof, and all Letters Patent of the United States which may be granted thereon and all reissues and extensions thereof, and all rights of priority under International Conventions and applications for Letters Patent which may hereafter be filed for said improvements in any country or countries foreign to the United States, and all Letters Patent which may be granted for said improvements in any country or countries foreign to the United States and all extensions, renewals and reissues thereof.

AND Metrix Services does hereby covenant and agree that it will communicate to the said ASSIGNEE, its successors, legal representatives and assigns, any facts known to it respecting said improvements, and testify in any legal proceeding, sign all lawful papers, execute all divisional, continuing and reissue applications, make all rightful oaths and generally do everything possible to aid the said ASSIGNEE, its successors, legal representatives and assigns, to obtain and enforce proper patent protection for said improvements in all countries.

IN TESTIMONY WHEREOF, Assignor intending to be legally bound has hereunto affixed his signature.



This 14 day of February, 2006

Signature of Hazim Ansari, CEO of Metrix Services

EXHIBIT C

DEPARTMENT OF THE NAVY
NAVAL RESEARCH LABORATORY
4555 OVERLOOK AVE SW
WASHINGTON DC 20375-5320

IN REPLY REFER TO

1004/620G
12 October 2006

Hazim Ansari
Network Signatures, Inc.
14252 Culver Dr., 914
Irvine, CA 92604

Re: Network Signatures' October 6, 2006 demonstration of EasyConnect™ at the Naval Research Laboratory (NRL)

Mr. Ansari,

Thank you for visiting NRL October 6th to demonstrate Network Signatures' EasyConnect™.

NRL's technical and legal personnel who attended the demonstration have considered Network Signatures' presentation and have determined that EasyConnect™ relates to an embodiment of the invention claimed in United States Patent No. 5,511,122 (the '122 patent) entitled "Intermediate Network Authentication."

Based on Network Signatures' demonstration, and absent any evidence to the contrary, NRL takes the position that Network Signatures has successfully carried out a plan for development of the licensed invention claimed the '122 patent and has brought an invention as recited in the '122 patent to practical application. So long as Network Signatures makes EasyConnect™ available to the public on reasonable terms, NRL will agree that Network Signatures has made the benefits of this invention reasonably accessible to the public, and therefore Network Signatures will be compliant with the first paragraph of Article III of the Exclusive License Agreement executed on September 28, 2004, and amended on February 14, 2006 (Agreement). NRL requests Network Signatures keep NRL informed regarding its commercialization and marketing activities as part of the annual reports Network Signatures will submit under Article IV of the Agreement.

I am also in receipt of your request that the Amendment to the Agreement be revised to reflect that Network Signatures is a Subchapter C corporation and not a Limited Liability Company (LLC). With your permission, I will make a "pen and ink" change on the Amendment to so reflect the proper status of Network Signatures.

EXHIBIT D

(17)

If you have any further questions and/or comments, please do not hesitate to contact the NRL Technology Transfer Office.

Sincerely,

Deirdre Zammit
Technology Transfer Office

US005511122A

# United States Patent [19]

Atkinson

[11] Patent Number: 5,511,122

[45] Date of Patent: Apr. 23, 1996

[54] **INTERMEDIATE NETWORK AUTHENTICATION**

[75] Inventor: Randall Atkinson, Annandale, Va.

[73] Assignee: The United States of America as represented by the Secretary of the Navy, Washington, D.C.

[21] Appl. No.: 256,087

[22] Filed: Jun. 3, 1994

[51] Int. Cl.[6] ..... H04K 1/00

[52] U.S. Cl. ..... 380/25; 380/23; 380/21; 380/30

[58] Field of Search ..... 380/23, 25, 30, 380/4, 49, 21

[56] References Cited

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 4,438,824 | 3/1984 | Mueller-Schloer | 380/23 |
| 4,965,827 | 10/1990 | McDonald . | |
| 5,175,765 | 12/1992 | Perlman . | |
| 5,204,907 | 4/1993 | Hershey et al. . | |
| 5,204,961 | 4/1993 | Barlow . | |
| 5,241,599 | 8/1993 | Bellovin et al. . | |
| 5,280,583 | 1/1994 | Nakayama et al. | 395/200 |
| 5,371,794 | 12/1994 | Diffie et al. | 380/21 |
| 5,416,842 | 5/1995 | Aziz | 380/30 |

OTHER PUBLICATIONS

Tsudik, Gene, "*Datagram Authentication in Internet Gateways: Implications of Fragmentation and Dynamic Routing*", IEEE Journal on Selected Areas in Communications, vol. 7, No. 4, (May, 1989), IEEE, NY, NY.

ISI, Transmission Control Protocol, RFC–793 Network Information Center, (Sep., 1981).

Voydock, V. L. and Kent, S. T., "*Security in High–Level Network Protocols*", IEEE Communications, vol. 23, No. 7 (Jul., 1985).

Rivest, R. & Dusse, S., "*The MD5 Message–Digest Algorithm*," RFC–1321, DDN Network Information Center (Apr., 1992).

Cole, Raymond, Jr. et al., "*Multilevel Secure Mixed–Media Communication Networks*," Proceedings of the 1989 IEEE Conference on Military Communications (MILCOM '89), IEEE, N.Y., N.Y.

Clark, D. D. and Wilson, "*A Comparison of Commercial and Military Computer Security Policies*," Proceedings of the 1987 IEEE Symposium on Security & Privacy, IEEE Computer Society, Oakland, California (1987).

NBS, FIPS PUB 46, "*Data Encryption Standard (DES)*," National Bureau of Standards, U.S. Department of Commerce (Jan., 1977).

Schneier, B., "*Applied Cryptography*," John Wiley & Sons, Inc., NY, NY (1994), p. 3.

Bellovin, Steven M., "Security Problems in the TCP/IP Protocol Suite" ACM, Computer Communications Review, vol. 19, No. 2 (Apr., 1989), pp. 32–48.

Bellovin, Steven M., "*Limitations of the Kerberos Authentication System*", Proceedings of the Winter 1991 Usenix Conference, Usenix Association, Berkley, CA (1991).

Kent, S. T. & Linn, J., Privacy Enhancement for Internet Electronic Mail: Part II–Certificate–based Key Management, RFC–1114, DDN Network Information Center (Aug., 1989).

Kent, S. T. US DoD Security Options for the Internet Protocol, RFC–1108, DDN Network Information Cen.

(List continued on next page.)

*Primary Examiner*—David C. Cain

*Attorney, Agent, or Firm*—Thomas E. McDonnell; Daniel Kalish

[57] **ABSTRACT**

An internetwork authentication method is provided for verifying a sending host by a receiving host or an intermediate router or gateway. The method comprises the steps of: obtaining a network address and a public key of a receiving host; utilizing the public key from the receiving host in combination with a private key of the originating host to generate a cryptographic signature; transmitting the signature along with data through a first subnetwork in at least one packet; receiving at least one packet at the receiving host; and the receiving host utilizing a private key of said receiving host site and a public key of said originating host to verify said cryptographic signature.

14 Claims, 4 Drawing Sheets

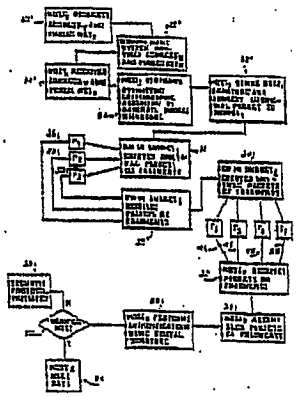
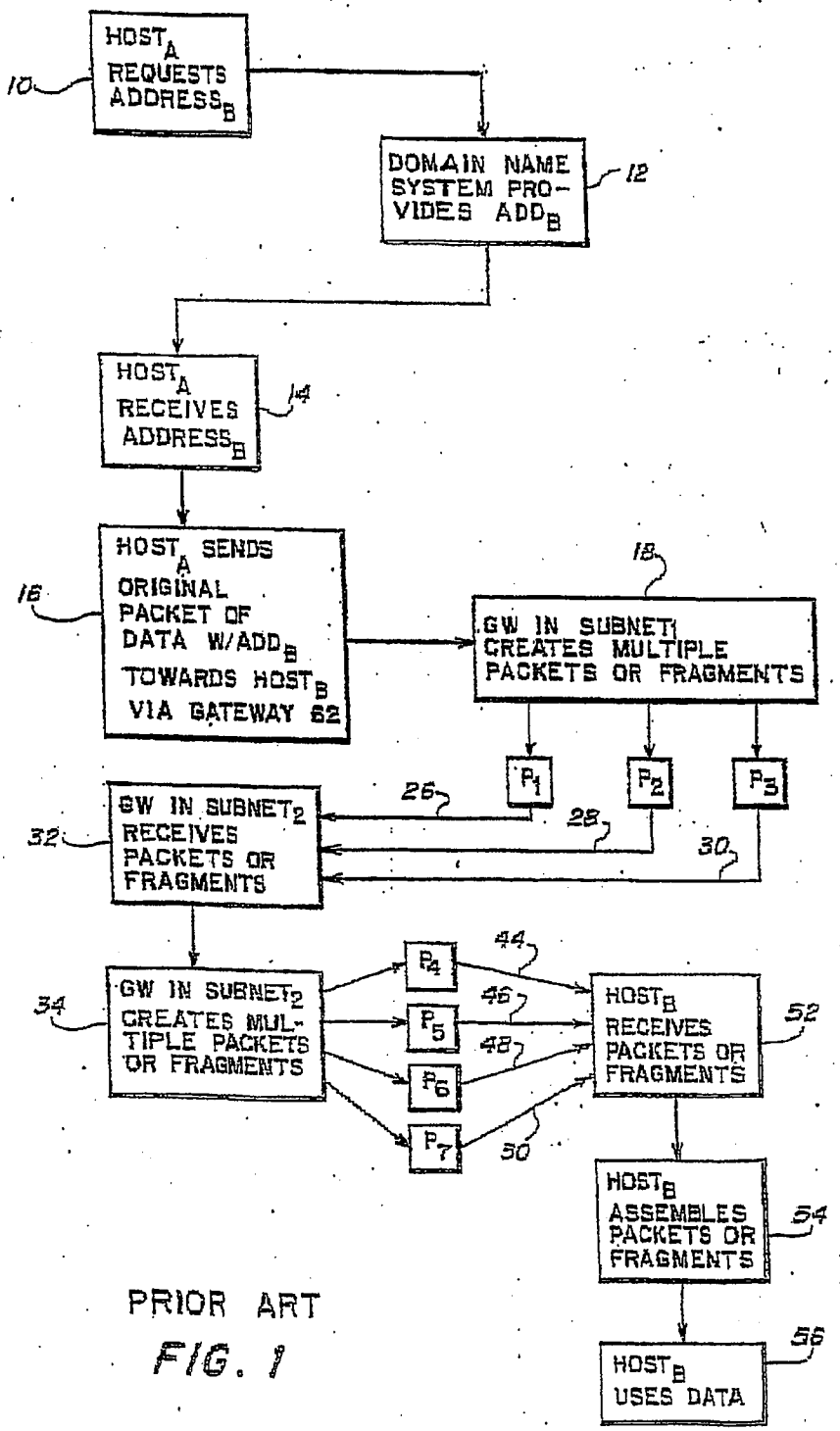


EXHIBIT B

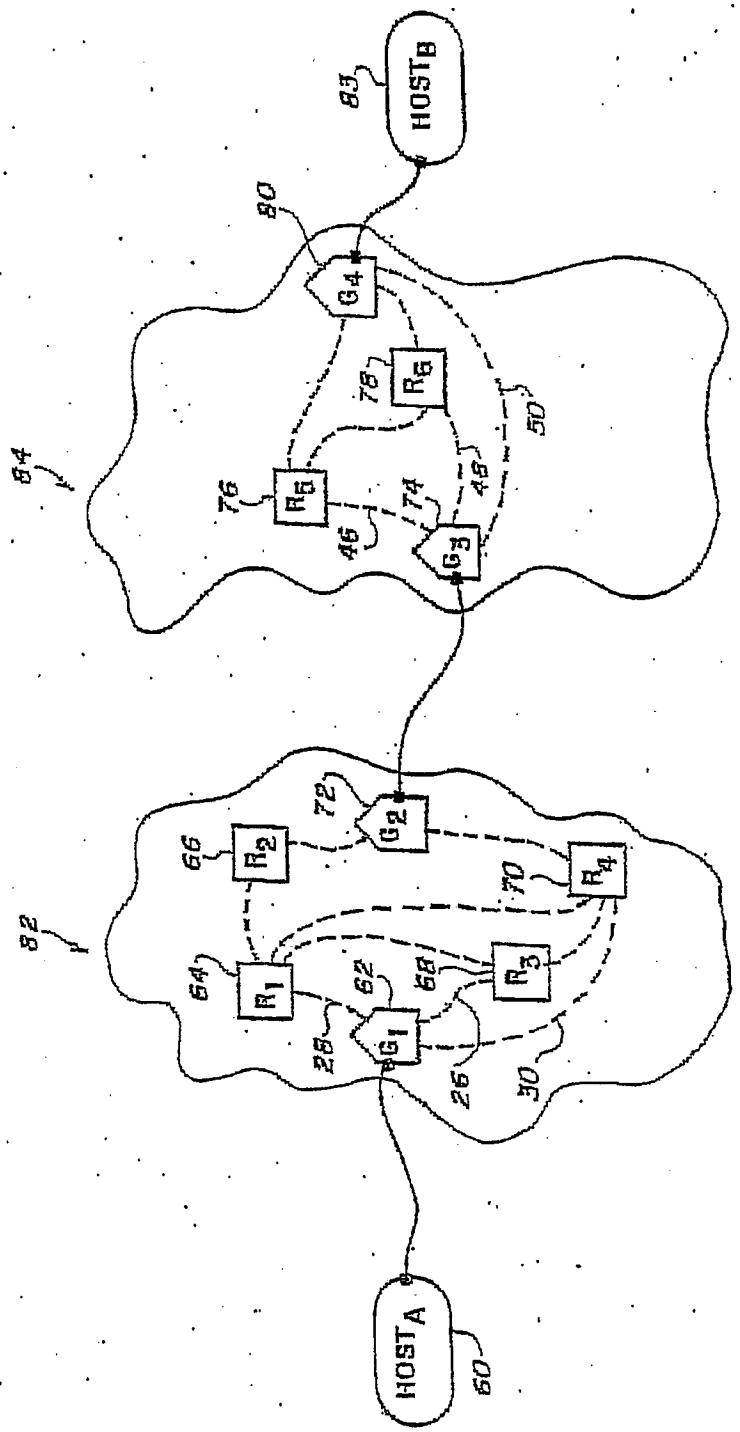
OTHER PUBLICATIONS

ter (Nov., 1991).
Mockapetris, Paul, Domain Names–Implementation and Specification, RFC–1035, DDN Network Information Center (Nov., 1987).
Needham, R. M. and Schroeder, M. D., *"Using Encryption for Authentication in Large Networks of Computers"*, Communications of the ACM, vol. 21, No. 12 (Dec., 1978).
*"Security Requirements for Cryptographic Modules"*, Federal Information Processing Standards Publication 140–1, (Jan. 11, 1994), pp. 1–53.
Braastad, Dennis et al., *"SP4: A Transport Encapsulation Security Protocol"*, Proceedings of 1987 NCSC Conference, pp. 158–161.
Nelson, Ruth, *"SDNS Services and Architecture"*, Proceedings of 1987 NCSC Conference, pp. 153–157.
Lambert, Paul A., *"Layer Wars: Protect the Internet with Network Layer Security"*, Motorola, Inc., Secure Telecommunications.
Dinkel, Charles (Editor), *"Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols"*, U.S. Dept. of Commerce, Nat'l. Inst. Stds., NISTIR 90–4250.




PRIOR ART

FIG. 1




PRIOR ART

FIG. 2

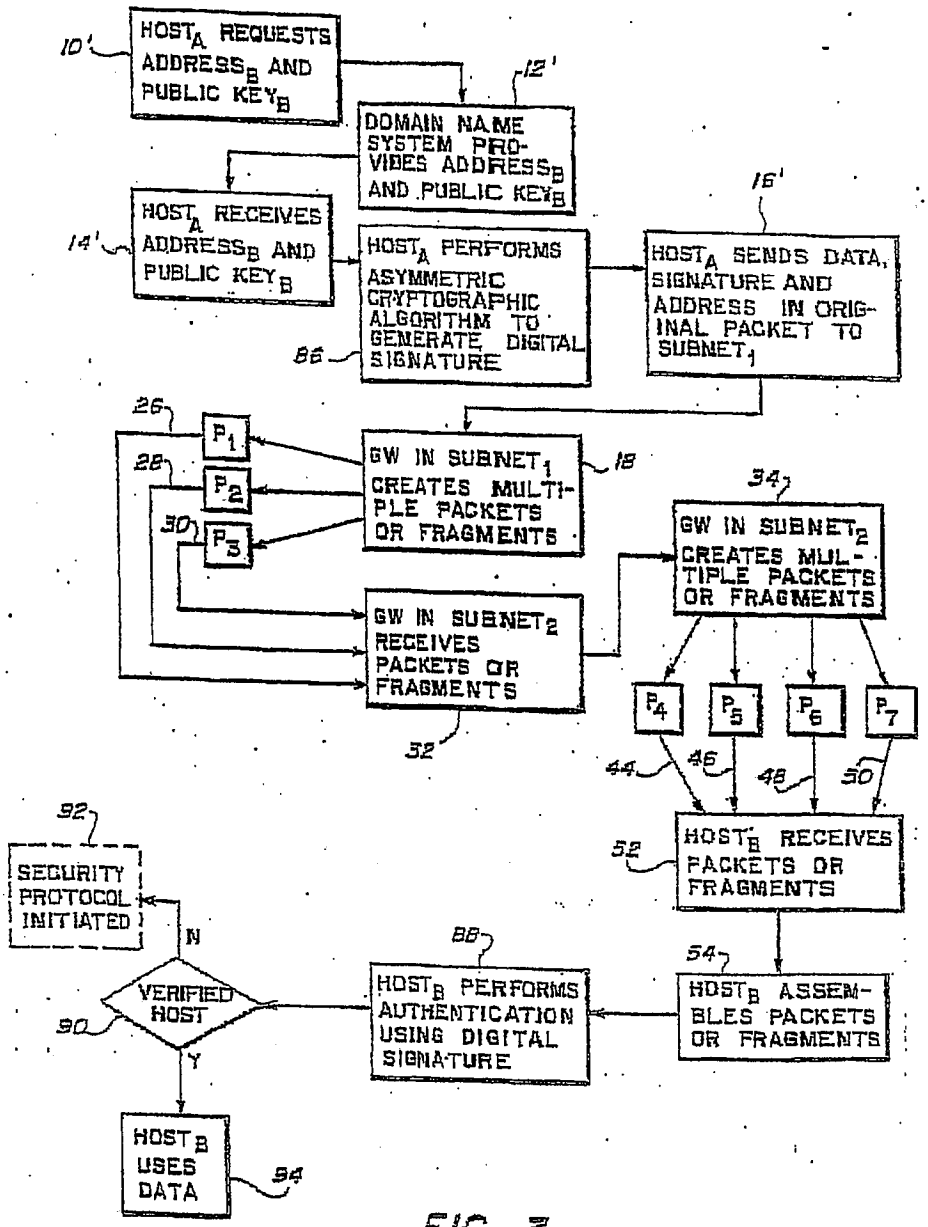

10'
HOST$_A$ REQUESTS ADDRESS$_B$ AND PUBLIC KEY$_B$
12'
DOMAIN NAME SYSTEM PROVIDES ADDRESS$_B$ AND PUBLIC KEY$_B$
14'
HOST$_A$ RECEIVES ADDRESS$_B$ AND PUBLIC KEY$_B$
HOST$_A$ PERFORMS ASYMMETRIC CRYPTOGRAPHIC ALGORITHM TO GENERATE DIGITAL SIGNATURE
86
16'
HOST$_A$ SENDS DATA, SIGNATURE AND ADDRESS IN ORIGINAL PACKET TO SUBNET$_1$
26
P$_1$
28
P$_2$
30
P$_3$
GW IN SUBNET$_1$ CREATES MULTIPLE PACKETS OR FRAGMENTS
18
GW IN SUBNET$_2$ RECEIVES PACKETS OR FRAGMENTS
32
34
GW IN SUBNET$_2$ CREATES MULTIPLE PACKETS OR FRAGMENTS
P$_4$
P$_5$
P$_6$
P$_7$
44
46
48
50
HOST$_B$ RECEIVES PACKETS OR FRAGMENTS
52
HOST$_B$ ASSEMBLES PACKETS OR FRAGMENTS
54
HOST$_B$ PERFORMS AUTHENTICATION USING DIGITAL SIGNATURE
88
VERIFIED HOST
90
N
Y
SECURITY PROTOCOL INITIATED
92
HOST$_B$ USES DATA
94

FIG. 3

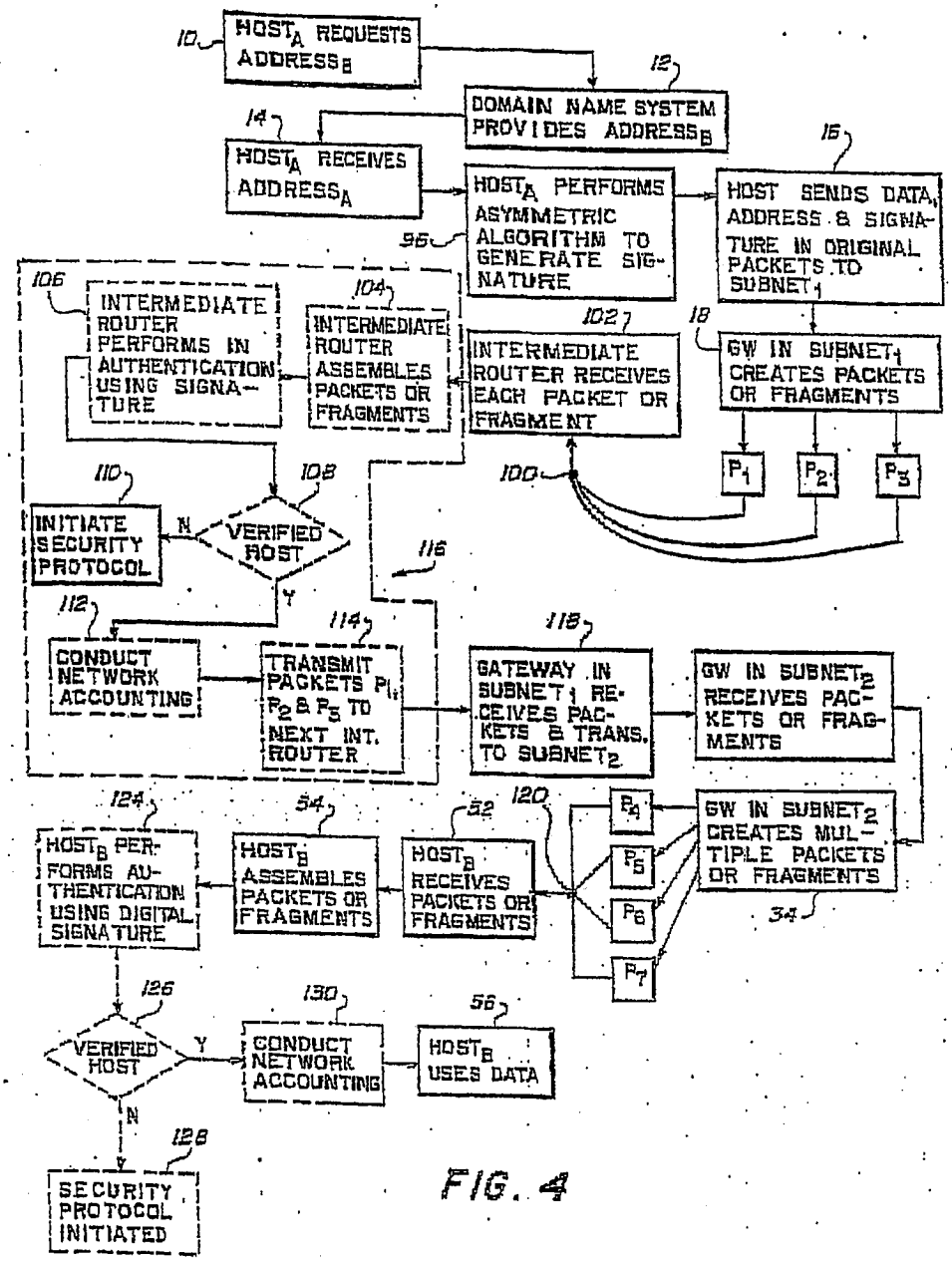

10
HOST$_A$ REQUESTS ADDRESS$_B$
12
DOMAIN NAME SYSTEM PROVIDES ADDRESS$_B$
14
HOST$_A$ RECEIVES ADDRESS$_A$
HOST$_A$ PERFORMS ASYMMETRIC ALGORITHM TO GENERATE SIGNATURE
96
16
HOST SENDS DATA, ADDRESS & SIGNATURE IN ORIGINAL PACKETS TO SUBNET$_1$
106
INTERMEDIATE ROUTER PERFORMS IN AUTHENTICATION USING SIGNATURE
104
INTERMEDIATE ROUTER ASSEMBLES PACKETS OR FRAGMENTS
102
INTERMEDIATE ROUTER RECEIVES EACH PACKET OR FRAGMENT
18
GW IN SUBNET$_1$ CREATES PACKETS OR FRAGMENTS
100
P$_1$
P$_2$
P$_3$
110
INITIATE SECURITY PROTOCOL
N
108
VERIFIED HOST
Y
116
112
CONDUCT NETWORK ACCOUNTING
114
TRANSMIT PACKETS P$_1$, P$_2$ & P$_3$ TO NEXT INT. ROUTER
118
GATEWAY IN SUBNET$_1$ RECEIVES PACKETS & TRANS. TO SUBNET$_2$
GW IN SUBNET$_2$ RECEIVES PACKETS OR FRAGMENTS
120
P$_4$
P$_5$
P$_6$
P$_7$
GW IN SUBNET$_2$ CREATES MULTIPLE PACKETS OR FRAGMENTS
34
124
HOST$_B$ PERFORMS AUTHENTICATION USING DIGITAL SIGNATURE
54
HOST$_B$ ASSEMBLES PACKETS OR FRAGMENTS
52
HOST$_B$ RECEIVES PACKETS OR FRAGMENTS
126
VERIFIED HOST
Y
130
CONDUCT NETWORK ACCOUNTING
56
HOST$_B$ USES DATA
N
128
SECURITY PROTOCOL INITIATED

FIG. 4

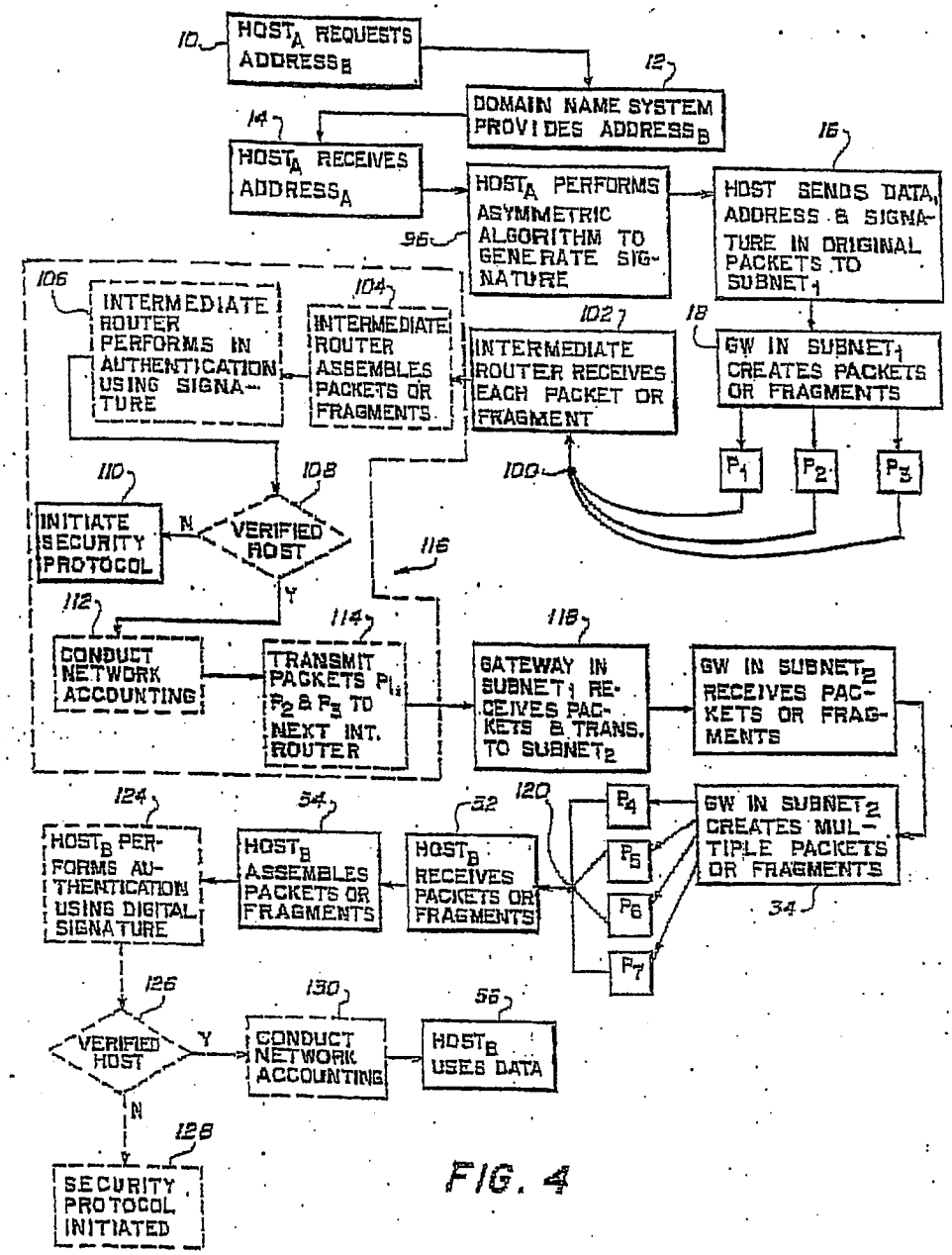

10
HOST$_A$ REQUESTS ADDRESS$_B$
12
DOMAIN NAME SYSTEM PROVIDES ADDRESS$_B$
14
HOST$_A$ RECEIVES ADDRESS$_A$
16
HOST$_A$ PERFORMS ASYMMETRIC ALGORITHM TO GENERATE SIGNATURE
96
HOST SENDS DATA, ADDRESS & SIGNATURE IN ORIGINAL PACKETS TO SUBNET$_1$
18
GW IN SUBNET$_1$ CREATES PACKETS OR FRAGMENTS
102
INTERMEDIATE ROUTER RECEIVES EACH PACKET OR FRAGMENT
104
INTERMEDIATE ROUTER ASSEMBLES PACKETS OR FRAGMENTS
106
INTERMEDIATE ROUTER PERFORMS IN AUTHENTICATION USING SIGNATURE
100
P$_1$
P$_2$
P$_3$
108
VERIFIED HOST
N
Y
110
INITIATE SECURITY PROTOCOL
112
CONDUCT NETWORK ACCOUNTING
114
TRANSMIT PACKETS P$_1$, P$_2$ & P$_3$ TO NEXT INT. ROUTER
116
118
GATEWAY IN SUBNET$_1$ RECEIVES PACKETS & TRANS. TO SUBNET$_2$
GW IN SUBNET$_2$ RECEIVES PACKETS OR FRAGMENTS
120
P$_4$
P$_5$
P$_6$
P$_7$
GW IN SUBNET$_2$ CREATES MULTIPLE PACKETS OR FRAGMENTS
34
52
HOST$_B$ RECEIVES PACKETS OR FRAGMENTS
54
HOST$_B$ ASSEMBLES PACKETS OR FRAGMENTS
124
HOST$_B$ PERFORMS AUTHENTICATION USING DIGITAL SIGNATURE
126
VERIFIED HOST
Y
N
130
CONDUCT NETWORK ACCOUNTING
56
HOST$_B$ USES DATA
128
SECURITY PROTOCOL INITIATED

FIG. 4

# INTERMEDIATE NETWORK AUTHENTICATION

## BACKGROUND OF THE INVENTION

The present invention relates generally to network security in a distributed network or between networks, and more particularly to an internetwork authentication method which is capable of intermediate authentication as well as authentication of fragmented data regardless of the network protocol.

Historically, most networking protocols and architectures have not included solid authentication or confidentiality mechanisms. The MIT Athena project has been the exception to this rule with its development of the Kerberos authentication system. This system is beginning to be implemented at some sites and some workstation manufacturers are considering implementing Kerberos in their standard OS releases, but the overwhelming majority of networked sites have no authentication or confidentiality mechanisms in their network architectures. The ISO (International Standards Organization) OSI (Open Standards Interconnection) suite provides for confidentiality services in the upper layers but does not require authentication of any of the lower layer protocols. These lower layer protocols have a number of security problems in protocols commonly used in the internet and have certain limitations intrinsic to the Kerberos protocols. The security issues in the ISO OSI suite appear to have gotten less attention than in the Internet suite because the Internet suite is more widely implemented at present.

Recently, the Internet Engineering Task Force has begun to incorporate authentication and confidentiality mechanisms in some protocols, notably the Simple Network Management Protocol (referred to as "SNMP") and Privacy Enhanced Mail. A few other recent protocol specifications, such as for the Border Gateway Protocol (referred to as "BGP") and Open Shortest Path First (referred to as "OSPF") routing protocols provide hooks for authentication to be added later but do not define or mandate any real authentication mechanism. The BGP version 3 specification explicitly states that the definition of authentication mechanisms other than the default "no authentication" option are out of the scope of the specification. Similarly, the OSPF version 2 specification asserts that "OSPF also provides for the authentication of routing updates, . . . " when in fact the only authentication mechanisms specified are "no authentication" or "clear-text password." Overall, there is no fundamental systemic security architecture in the Internet protocol suite at present.

Bellovin, in his article entitled "Security Problems in the TCP/IP Protocol Suite" ACM Computer Communications Review, Vol. 19, No. 2 (April 1989), pp. 32–48 identifies that there are security flaws in the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite because hosts rely on IP source address for authentication and also because routing protocols have minimal to no authentication. The Bellovin article is incorporated herein by reference. Similarly, the ISO protocol has not paid sufficient attention to building security mechanisms into the network, transport, or routing protocols.

Some proposed computer security policies, such as Clark-Wilson, are not practical to implement using current network protocols, which rely on datagram fragmentation, unless intermediate authentication is provided. For a discussion of such policies, see D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," Proceedings of the 1987 IEEE Symposium on Security & Privacy, IEEE Computer Society, Oakland, Calif. (1987), which is incorporated herein by reference.



Aside from concerns about attacks, there is recently much interest in implementing policy-based routing, network usage accounting, and network auditing. None of these may be dependably implemented unless the network protocol headers may be authenticated by routers as well as the end hosts. If there is no intermediate authentication, then it is straight forward to spoof policy-based routing and to cause others to pay for one's network traffic. Without authentication, auditing cannot yield meaningful results. It is clear that network protocol header authentication is essential for both existing and future services.

Thus, there is a need for providing intermediate authentication in networking. By being able to authenticate a packet while in route, the possibility of host masquerading and network attacks are reduced. Additionally, policy-based routing, network usage accounting, and network auditing may be implemented.

## SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an authentication method which will provide for both intermediate authentication as well as host to host authentication in a datagram network that permits fragmentation of datagrams.

It is a further object to provide an accurate method for determining the network traffic generated by a particular host.

It is yet another object to provide a means for accurately billing a host for its use of network traffic and facilities.

It is yet another object to provide for detection of a non-valid host on a network.

It is yet another object to improve network reliability as well as network security.

It is yet another object to provide support for network auditing, network traffic counting, and policy based routing.

In all of the above embodiments, it is an object to provide an authentication system which utilizes an asymmetric key system in the authentication system.

It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of the first packet fragment or datagram fragment.

According to one broad aspect of the present invention, there is provided a method for network authentication comprising the steps of: obtaining a network address and a public key for a receiving host; utilizing the public key from the receiving host in combination with a private key from the sending host to generate a cryptographic signature; transmitting the signature along with data through a first subnetwork in at least one packet; receiving at least one packet at the receiving host; and the receiving host utilizing a private key for said receiving host site and a public key for said sending host to verify said cryptographic signature.

According to another broad aspect of the invention, there is provided a method for network authentication of fragmented packets comprising the steps of: requesting a network address for a receiving host from a subnetwork name system; utilizing a private key from a sending host to generate a cryptographic signature; transmitting the signa-

ture along with data to a first subnetwork in at least one packet, having a first packet size which is different from that of the transmitting host and thereby fragmenting the original packet into at least two packet fragments, the packet fragments having a first packet fragment which is transmitted to a first available intermediate gateway or router in the first subnetwork, and each subsequent fragment of that first packet fragment following the progress of the first packet fragment through the first subnetwork in a train-like fashion; reassembling the fragmented packets at an intermediate gateway or router; performing a verification of the cryptographic signature on the reassembled packet; retransmitting the fragmented packets through the first subnetwork; receiving at least one packet at the receiving host; and utilizing a public key for the sending host to verify the cryptographic signature.

By being able to provide both host to host authentication as well as intermediate authentication, the possibilities of host masquerading and network attacks are reduced or eliminated. Additionally, policy-based routing, network usage accounting, and network auditing may be implemented.

Other objects and features of the present invention will be apparent from the following detailed description of the preferred embodiment.

## BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be further described in conjunction with the accompanying drawings, in which:

FIG. 1 is a flow chart illustrating a method utilized in a typical or prior art communications transaction between $host_A$ and $host_B$ in which no authentication is conducted in a network which may employ fragmentation of datagrams;

FIG. 2 is an exemplary network topography of communications between $host_A$ and $host_B$ according to the prior art;

FIG. 3 is a flow chart illustrating a first preferred communications transaction between $host_A$ and $host_B$ in which end to end authentication is conducted in a network which may employ fragmentation of datagrams; and

FIG. 4 is a flow chart illustrating a second preferred communications transaction between $host_A$ and $host_B$ in which both intermediate and end to end authentication may be conducted in a network which may employ fragmentation of datagrams.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference to the Figures, wherein like reference characters indicate like elements throughout the several views and, in particular, with reference to FIGS. 1 and 2, a generic method of host to host communication is illustrated. In order to appreciate the improvements associated with the invention disclosed herein, a detailed description of the prior approach to network communication is essential.

In prior network communication applications, a host, generically referred to as $host_A$ or element 60 will wish to communicate with a $host_B$ or element 83. $Host_A$ 60 may be in the same subnetwork or network as $host_B$ 83 or may be in a different subnetwork or network. $Network_1$ 82 is the network containing $host_A$ 60 and $network_2$ 84 is the network containing $host_B$ 83. FIGS. 1 and 2 illustrate the condition where $host_A$ 60 and $host_B$ 83 are in different subnetworks. When $host_A$ 60 wishes to communicate with $host_B$ 83, $host_A$ 60 will obtain the address and key of $host_B$ 83 from a network name system via the networks or from a configuration table at $host_A$ 60. This request is illustrated by box 10 in FIG. 1. The network name system will provide the network address of $host_B$ 83 to $host_A$ 60 as illustrated by box 12. Next, the network address is received by $host_A$ 60, see box 14. After receiving the address, $host_A$ 60 begins to transmit datagrams or packets towards $host_B$ 83 via a gateway 62, see box 16. The physical communication protocol being used between $host_A$ 60 and $subnetwork_1$ 82 will vary with the particular type of host and network. The above described method is one of several well known methods for obtaining the network address of a host.

$Subnetwork_1$ 82, as illustrated by box 18, will then process data into packets which are link or subnetwork specific. A standard protocol which is utilized is the IP. In this protocol, datagrams or packets are formed from the data stream. Packets generally comprise a header section, a data section and a trailer section. The specific relationship between these sections or the existence of these sections are protocol specific and thus will not be discussed in any detail. The data may be fragmented by the creation of packets for $subnetwork_1$ 82 and thereby take different routes through $subnetwork_1$ 82 towards $host_B$ 83. For illustrative purposes, three packets or fragmented packets, $P_1$, $P_2$ and $P_3$ are illustrated. These packets are transmitted through $subnetwork_1$ 82 by a conventional transmission method. Each packet or fragment may take a different route through the subnetwork as illustrated by lines 26, 28 and 30 which correspond to the routes of packets $P_1$, $P_2$ and $P_3$, respectively. Thus, each packet may go through a different intermediate router 64, 66, 68 or 70 as illustrated in FIG. 2.

U.S. Pat. No. 5,175,765 to Perlman is exemplary of the drawbacks of the prior art. Perlman discloses an authentication system which utilizes an asymmetric key system to authenticate a data packet. This system utilizes a robust broadcasting technique and therefore is not capable of performing intermediate fragmentation or intermediate authentication for the reasons discussed above. Both of these capabilities are important for proper network usage accounting.

Eventually, packets $P_1$, $P_2$ and $P_3$ will migrate through $subnetwork_1$ 82 along the dashed lines in FIG. 2. In a configuration not shown, if $host_B$ 83 were located within $subnetwork_1$ 82, $host_B$ 83 would receive the packets and reassemble them to gain access to the data contained therein. $Host_B$ 83 would utilize this data and will assume that the sender, $host_A$ 60, is the actual sender of the data. Thus, there would not be any end to end or intermediate authentication of the host or data. In this situation, the data would be fragmented only one time, i.e., during the creation of packets $P_1$, $P_2$ and $P_3$.

In the configuration shown in FIG. 2, $host_B$ 83 is located in a different subnetwork, $subnetwork_2$ 84 than $subnetwork_1$ 82. Packets $P_1$, $P_2$ and $P_3$ will be transmitted from gateway 72 of $subnetwork_1$ 82 to gateway 74 of $subnetwork_2$ 84. This step is illustrated in FIG. 1 as block 32. The link/subnetwork protocols utilized in $subnetwork_1$ 82 may differ from those of $subnetwork_2$ 84. In this situation, $subnetwork_2$ 84 will create additional packets $P_4$, $P_5$, $P_6$ and $P_7$, see block 34. Four packets have been used for illustrative purposes only but any number of packets may be generated by $subnetwork_2$ 84. Since the link or subnetwork protocols of $subnetwork_1$ 82 and $subnetwork_2$ 84 may be different, the size of the packets may also be different. Thus, the original data, header and trailer information of each packet in $subnetwork_1$ 82 may now appear in different packets in $subnetwork_2$ 84, i.e., the information from packet $P_1$ may now be contained

between packets $P_4$ and $P_5$. Thus, the data has been fragmented for a second time. Packets $P_4$, $P_5$, $P_6$ and $P_7$ are transmitted through the intermediate routers 76 and 78 of subnetwork$_2$ 84 along the dashed lines of subnetwork$_2$ 84 and in a similar fashion to that of subnetwork$_1$ 82 above. There may be any number of intermediate routers and those used in FIG. 2 are for illustrative purposes only. Lines 44, 46, 48 and 50 illustrate the transmission concept in FIG. 1.

In such a technique, the ability to authenticate packets at an intermediate gateway or router, such as router 76, is completely lost since each packet fragment may take a different route through subnetwork$_2$ 84. Additionally, since the information contained in packet $P_1$ may be split between packets $P_4$ and $P_5$, it is impossible to assemble the information of packet $P_1$ at an intermediate gateway or router. In this situation, the original data is fragmented two times, i.e., once when packets $P_1$, $P_2$ and $P_3$ are created and once when packets $P_4$, $P_5$, $P_6$ and $P_7$ are created.

Eventually, packets $P_4$, $P_5$, $P_6$ and $P_7$ will migrate through subnetwork$_2$ 84 along the dashed lines in FIG. 2. Host$_B$ 83 will receive the packets and reassemble them to gain access to the data contained therein, see blocks 52 through 56. Host$_B$ 83 will utilize this data and will assume that the sender, host$_A$ 60, is the actual sender of the data. Thus, there is no end to end or intermediate authentication of the host or data.

Several U.S. Patents have touched on the subject of authentication. For example, U.S. Pat. No. 4,965,827 to McDonald discloses an authentication algorithm for verifying that a message has not been corrupted or changed during transmission. This method utilizes a symmetric cryptographic hash function which is only used for the authentication of the data. In a symmetric key system, the same key is used for encryption and decryption and does not provide the protection of an asymmetric key system. The McDonald system provides no means for authenticating that a particular host has actually sent the data. Thus, a host may masquerade as a valid host and send invalid data over the network. Additionally, network applications including intermediate authentication are not described by the McDonald patent. As another example of a U.S. Patent discussing authentication, U.S. Pat. No. 5,241,599 to Bellovin et al., discloses a key management protocol which could be used over a network which is not secure.

The above description provides a basic understanding of how data is transferred between host$_A$ 60 and host$_B$ 83. Now we will turn to a new method of host authentication as illustrated in FIGS. 3 and 4. FIG. 3 illustrates a host to host authentication method and FIG. 4 illustrates a host to intermediate gateway or router authentication method. Like reference numerals have been utilized where there is no significant difference between the invention and the prior art. Primes above the reference numerals have been utilized where the elements are similar to the prior art but have additional features or modifications. Finally, new reference numerals are provided for new steps which are conducted.

## Cryptographic Method

Before a description of the new methods are provided, it is necessary to describe current cryptographic mechanisms. Cryptographic mechanisms provide the greatest assurance of the authenticity of data. Cryptographic systems come in two varieties, symmetric key and asymmetric key. See, B. Schneier, "Applied Cryptography," John Wiley & Sons, Inc., New York, N.Y. (1994), p.3, which is incorporated herein by reference. In a symmetric key system, the same key is used for encryption and decryption. When providing confidentiality using an asymmetric system, each party has two keys, one public and one private, and data is usually encrypted using the sender's private key and the recipients public key. When providing authentication using an asymmetric system, the data and the keys are used to generate a digital signature. That signature is verified by the recipient using the data received and the appropriate decryption keys.

## Host to Host Authentication

Turning now to FIG. 3, the steps involved in a new method of host authentication are illustrated. A host, generically referred to as host$_A$ or element 60 will wish to communicate with a host$_B$ or element 83. Host$_B$ 83 may be in the same subnetwork or network 82 as host$_A$ 60 or may be in a different subnetwork or network 84. FIGS. 1 and 2 illustrate the condition where host$_A$ 60 and host$_B$ 83 are in different subnetworks, 82 and 84, respectively. When host$_A$ 60 wishes to communicate with host$_B$ 83, host$_A$ 60 will request the address and public key of host$_B$ 83 from a subnetwork name system. This request is illustrated by box '10' in FIG. 3. The public key request is important in this new method and its importance will be discussed in detail below.

## Subnetwork Name System

It is possible to distribute the public keys to all hosts and users of the internetwork, see Mockapetris, Paul, Domain Names—Implementation and Specification, RFC-1035, DDN Network Information Center (November, 1987) which is hereby incorporated by reference. Public keys for hosts are included in the nameservice database and all nameservice responses are authenticated. This means that all of host public keys are distributed in an authenticated manner. Name service requests need not be authenticated or confidential in the general case. However, if the visibility of some data in the nameservice database is to be controlled, then authenticated confidential requests would be required to access non-published data and authenticated confidential responses to such requests would also be required. The public keys for the root nameservers should be made readily available, such as by telephone and postal mail, so that system administrators may have confidence in the authenticity of the root public key. Otherwise, if the correct root public key were not widely known, an intruder would be easily able to masquerade as the legitimate nameserver.

Because the user and application level keys are distributed using mechanisms implemented in the local host, those keys may be changed easily by the user without much concern for the key change being delayed in propagation to all of the directory or network name service providers. Host keys are less easily changed, but such changes should be regularly scheduled in order to limit damage from compromised keys.

## Modifications To Current Protocol

This section described additions and changes to the Internet Protocol suite to enable its use to distribute asymmetric keys and to enable its responses to be authenticated.

A new TYPE field is added to the resource records in the Domain Name System. This new field contains a signed asymmetric host authentication key to be used by hosts attempting to authenticate network packets. Each host which transmits any authenticated frames must have this record in the Domain Name System (referred to as "DNS") and the value of the record must be correctly advertised. The pro-

posed name of this new DNS record type is HAK. The value of the HAK is represented as hexadecimal numbers using the digits 0 through 9 and letters A through F. The HAK record's value is the authentication key certificate used for that host that the HAK record is associated with. No HAK records may exist that are not associated with a specific host.

All Subnetwork Name System responses from nameservers provide authentication. All Subnetwork Name System requests should provide authentication. Hosts receiving an unauthenticated response should take note of the lack of authentication and may ignore unauthenticated responses if required by the security policy applicable to the subnetwork of the receiving host or take appropriate action. Hosts receiving a response containing incorrect authentication data should discard the response without processing it further.

To provide user asymmetric keys for encryption or authentication, it is suggested that a new service, the Key Information Protocol or KIP, be provided. This service would accept requests for user public keys and would respond only if such information were available. The "no key exists for that user" and "that user not valid here" cases would both cause an "invalid request" to be sent back to the requestor. All responses would use IP authentication. The Key Information Protocol would also use the host's public authentication key in the KIP response to enable the recipient to authenticate the response. KIP should provide for separate authentication and confidentiality keys. Depending on perceived need, KIP could even be extended to use a Needham & Schroeder-like mechanism to set up and use symmetric keys for some session with the two KIPs handling the key set up securely (each on behalf of its local user) See, Needham, R. M. and Schroeder, M. D., "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM, Vol. 21, No. 12 (December 1978), pages 993–999, which is incorporated herein by reference. The use of the Needham & Schroeder-type symmetric key mechanism is less desirable than using asymmetric key technology because of the increased complexity.

When the KIP concept is implemented, a new Domain Name System record should be added that would point to the name of the host providing KIP service for a host or subnetwork.

Turning back to the steps in the host to host authentication method illustrated in FIG. 3, the subnetwork name system will provide either the name of the nameserver for the subnetwork containing the desired host or the public key and address of the desired host. All responses would be authenticated using the public key of the nameserver and any unauthentic responses would be discarded, and ignored. It might be valuable to audit all unauthentic responses. This process would be repeated as necessary until the requesting host received an authentic response containing the public key and address of the desired other host. If the locally trusted nameserver uses caching of data, response time would be reasonable despite having authentication. Using local nameservers and caching is a good implementation strategy for nameservice regardless of whether authentication is used. This process of the subnetwork name server getting and sending the address and public key is illustrated by box 12'.

As shown in box 14', the network address and public key information is next received by $host_A$ 60. At this point, $host_A$ 60 uses an asymmetric cryptographic algorithm to generate a digital signature, see box 16. As discussed further below, the public key of $host_B$ 83 is used in combination with the private key of $host_A$ 60 to generate a digital signature.

Asymmetric Algorithm

An asymmetric algorithm is utilized to generate a digital signature. This may be accomplished in several ways. The first method is to utilize a well known asymmetric algorithm such as RSA. See, U.S. Pat. No. 4,405,829 to R. L. Rivest, A. Shamir and L. M. Adleman, which is incorporated herein by reference. A second method is to encrypt the output of a symmetric cryptographic hash function using an asymmetric encryption algorithm. A third method is to use a keyed asymmetric cryptographic hash algorithm. The above three methods have been utilized in the past to provide end-to-end application-layer authentication but have not been used to provide intermediate network authentication. There is a significant difference between authenticating the accuracy of transmitted data, i.e. application-layer authentication, and network-layer authentication, the subject matter of this application. For convenience, the output of the asymmetric algorithm will be referred to as a digital signature.

Confidentiality and authentication might also be built into applications above the transport layer or into the transport layer itself. In some cases, it might be desirable to also use mechanisms built into the upper layer protocol that are independent of these network-layer mechanisms. For example, the Secure SNMP specifications build authentication and optional confidentiality mechanisms into the SNMP applications. This approach has the advantage that a security breach at a higher layer does not necessarily compromise the security at the network layer. However, security above the network layer does not provide authentication or confidentiality to all network users or applications and is not a general approach. For examples of transport-layer protocols, see ISI, Transport Control Protocol, RFC-793 Network Information Center (September, 1981) and ISI, OSI Transport Protocol Specification, IS-8073, ISO (1986), both of which are hereby incorporated by reference.

The next question is what will the asymmetric algorithm be used on, i.e., the data, the header information or the entire network protocol frame. It makes more sense to authenticate the entire network protocol frame than the header data alone. The incremental cost of authenticating the entire frame instead of just the headers is not significant and the increased entropy and size of the authenticated information makes many cryptanalytic attacks on the authentication harder, while also ensuring the authenticity of the data. Bellovin, in "Security Problems in the TCP/IP Protocol Suite" (supra) described a number of attacks at the transport layer, such as using TCP sequence number prediction to masquerade as another host's connection. Even trustworthy hosts need to isolate user connections from one another and to ensure that no user is capable of masquerading as another user via networking mechanisms. The ability to provide circuit-oriented confidentiality mechanisms is also desirable. Neither TCP nor OSI transport protocol currently provides either authentication or confidentiality mechanisms, which is the area of this disclosure, although the U.S. Government has published a standard called SP4 that adds security to TCP and an ISO OSI Transport Protocol.

While it is possible to support transport authentication using entirely different mechanisms than those used to provide network authentication, it is desirable to devise a common approach to authentication so that the overhead of implementation is minimized and so that the different services integrate together nicely. Moreover, there is a potential for decreased size in the trusted code required to implement the authentication services. It is usually easier to verify the correctness and trustworthiness of smaller amounts of code than larger amounts of code.

Turning back to the steps in the host to host authentication method illustrated in FIG. 3, after performing the asymmetric encryption, $host_A$ 60 begins to transmit data, address and the digital signature to $subnetwork_1$ 82 via a gateway 62, see box 16. The link/subnetwork communication protocol being used between $host_A$ 60 and $subnetwork_1$ 82 may vary with the particular type of host and network and thus, the location of the signature may vary.

$Subnetwork_1$ 82, as illustrated by box 18, will then process data into packets or fragments which are network or subnetwork specific. For illustrative purposes, three packets or, $P_1$, $P_2$ and $P_3$ are illustrated. Packets generally comprise a header section, a data section and a trailer section. The specific relationship between these sections or the existence of these sections are protocol specific and thus will not be discussed in any detail. The location of the signature may be in any of the above identified packet sections. These packets are transmitted through $subnetwork_1$ 82 by a conventional transmission method. The packets may also be routed as will be discussed in relation to the intermediate authentication method, below. Each packet or fragment may take a different route through the network as illustrated by lines 26, 28 and 30 which correspond to the routes of packets $P_1$, $P_2$ and $P_3$, respectively. Thus, each packet may go through a different intermediate router 64, 66, 68 or 70 as illustrated in FIG. 2.

An intermediate router is any device which routes packets between any two communication devices. A gateway is an intermediate router which connects two subnetworks. Therefore, the terms may be used interchangeably throughout the detailed description.

Eventually, packets $P_1$, $P_2$ and $P_3$ will migrate through $subnetwork_1$ 82 along the dashed lines in FIG. 2. In an architecture not shown, in which $host_B$ 83 is located within $subnetwork_1$ 82, then $host_B$ 83 will receive the packets or fragments and reassemble them to gain access to the data and signature contained therein. $Host_B$ 83 will utilize a corresponding asymmetric algorithm to decode or verify the signature and thereby verify the authenticity of $host_A$ 60. This is accomplished by utilizing the public key of $host_A$ 60 in combination with the private key of $host_B$ 83, see the discussion on encryption above.

If $host_B$ 83 is located in another subnetwork 84, as illustrated in FIG. 2, then packets $P_1$, $P_2$ and $P_3$ will be transmitted from gateway 72 of $subnetwork_1$ 82 to gateway 74 of $subnetwork_2$ 84. This step is illustrated in FIG. 3 as block 32. The link/subnetwork protocols utilized in $subnetwork_1$ 82 may differ from that of $subnetwork_2$ 84. In this situation, $subnetwork_2$ 84 will create additional packets or fragments $P_4$, $P_5$, $P_6$ and $P_7$, see block 34. Four packets have been used for illustrative purposes only and any number of packets may be generated by $subnetwork_2$ 84. Since the protocols of $subnetwork_1$ 82 and $subnetwork_2$ 84 may be different, the size of the packets may also be different. Thus, the original signature, data, header and trailer information of each packet in $subnetwork_1$ 82 may now appear in different packets in $subnetwork_2$ 84, i.e., the information from packet $P_1$ may now be contained between packets $P_4$ and $P_5$. As stated above, packets $P_4$, $P_5$, $P_6$ and $P_7$ are transmitted through the intermediate routers 76 and 78 of $subnetwork_2$ 84 along the dashed lines of $subnetwork_2$ 84 and in a similar fashion to that of $subnetwork_1$ 82 above. Optionally, the packets may be transmitted in a manner similar to that explained for the intermediate authentication method below. There may be any number of intermediate routers and links between routers and those used in FIG. 2 are for illustrative purposes only. Lines 44, 46, 48 and 50 illustrate the general transmission concept in FIG. 3.

The ability to authenticate packets at an intermediate gateway or router, such as router 76, is not a concern in a host to host authentication method.

Eventually, packets $P_4$, $P_5$, $P_6$ and $P_7$ will migrate through $subnetwork_2$ 84 along the dashed lines in FIG. 2. $Host_B$ 83 will receive the packets and reassemble them to gain access to the signature data contained therein, see blocks 52 and 54. $Host_B$ 83 will utilize a corresponding asymmetric algorithm to decode or verify the signature and thereby verify the authenticity of $host_A$, see block 88. This is accomplished by utilizing the public key of $host_A$ 60 in combination with the private key of $host_B$ 83, see the discussion on cryptographic algorithms above. If $host_A$ is authentic, then the data will be utilized by $host_B$ 83. Otherwise, a security protocol may be initiated to notify a network official of a potential security problem, see block 92.

## Intermediate Authentication

Turning now to FIG. 4, a method for intermediate authentication is illustrated. This method is very similar to that of the host to host authentication as described above. Therefore, only the differences between the two methods will be discussed in detail.

In order to permit any intermediate network gateway or router to authenticate the contents of the network frame, the public key for each host is published and the private key is kept private by that host. The sending $host_A$ 60 uses its public encryption key plus the data to generate a cryptographic signature which is embedded in the packet, see block 96. In this method, the public key of $host_B$ 83 is not requested or utilized in any manner.

Network frames are frequently fragmented into smaller frames that will fit within the size limitation of the protocols in and underneath the link or subnetwork layer. Thus, the original frames may be fragmented, i.e., packets $P_1$, $P_2$ and $P_3$ may be different in size than the ones originally transmitted by $host_A$ 60 to $subnetwork_1$ 82. In most cases currently, reassembly only occurs at the destination node and has drawbacks with respect to performance degradation associated with packet fragment reassembly. Intermediate nodes, such as routers or gateways, need not pay the reassembly cost unless they wish to perform intermediate authentication. Note that the original network packets may still be routed independently and dynamically and thus this new technique is still very flexible. When the packets migrate from one subnetwork to another, the packets may be reassembled into the original packets and then be transmitted as the original packets, thereby avoiding additional fragmentation and allowing for dynamic routing of the original packets in the current subnetwork.

These packet fragments are introduced to $subnetwork_1$ 82 as described above. The fragments are transmitted through $subnetwork_1$ 82 in a very different manner. The first fragment of each original packet to be transmitted is sent to the first available intermediate router in a conventional fashion. Each subsequent fragment of the original packet will then follow the same route as the first fragment through $subnetwork_1$ 82. This method is significantly different than the transmission scheme which is utilized in the prior art. Thus, the packet fragments form a train through $subnetwork_1$ 82 as illustrated in FIG. 4 by point 98 and line 100. Each original packet is routed conventionally unless the original packet is fragmented. In the case when the packet is fragmented, each packet fragment will traverse the same route as its first fragment.

At this stage, the intermediate router may decide to authenticate the packet fragment information. The decision on when and how often to authenticate will be a policy decision and will vary between subnetworks. If the intermediate router does perform authentication, then the intermediate router will assemble the packet fragments $P_1$, $P_2$ and $P_3$, see dashed box 104. This step is necessary since the original packets have been fragmented, i.e. packets $P_1$, $P_2$ and $P_3$ are different in size than the ones originally transmitted by $host_A$ 60 in subnetwork$_1$ 82. Then the intermediate router reads the reassembled packet to determine the sender's identity and attempts to confirm that the claimed sender's published public key produces the correct results when applied to the embedded digital signature, see dashed boxes 106 and 108. If there is a correct result from the asynchronous algorithm, then the sender and the data are authentic. Otherwise, the sender or some part of the data is not authentic. This permits policy-based routing and usage-based accounting to be dependably implemented as illustrated in dashed box 112. Finally, the intermediate router transmits the reassembled packet to the next router or gateway, possibly refragmenting the packet if necessary, see dashed box 114. The above process may be repeated by each intermediate router or gateway and is illustrated by dashed block 116. Note that the reassembled packets may still be routed independently and dynamically and so the new technique retains flexibility.

The packet fragments are eventually received by subnetwork$_2$ 84 as described above. As stated previously, there may be a second fragmentation problem which may occur when packets $P_4$, $P_5$, $P_6$ and $P_7$ are formed. One must have the entire original network frame intact in order to attempt to authenticate it. Network frames are frequently fragmented into smaller frames that will fit within the size limitation of the protocols in and underneath the link or subnetwork layer as illustrated by packets $P_4$, $P_5$, $P_6$ and $P_7$. This means that at each point where a router or gateway wishes to attempt to authenticate the network packet, it must reassemble all of the components of the original network packet first. It also means that if any intermediate router or gateway does not reassemble the original frame before resending or resending different fragments of a given network packet over different routes, that intermediate routers or gateways downstream from that gateway or router will be unable to authenticate the fragmented network packets.

In most cases currently, reassembly only occurs at the destination node. Intermediate nodes, such as routers or gateways, do not currently pay this cost. Reassembly and potential subsequent refragmentation will impair software performance when the link and physical protocols carry very small amounts of data in each lower level frame. This imposition may be reduced by utilizing appropriate hardware. Commercially available routers commonly have such hardware.

Any gateway or router in subnetwork$_2$ 84 is capable of intermediate authentication by executing the steps illustrated in dashed block 116.

Eventually, packets $P_4$, $P_5$, $P_6$ and $P_7$ will migrate through subnetwork$_2$ 84 along the dashed lines in FIG. 2. $Host_B$ 83 will receive the packets and reassemble them to gain access to the signature data contained therein, see blocks 52 and 54. $Host_B$ 83 will utilize a corresponding asymmetric algorithm to decode or verify the signature and thereby verify the authenticity of $host_A$, see block 124. This is accomplished by utilizing the public key of $host_A$ 60, see the discussion on encryption above. If $host_A$ is authentic, then network accounting will take place and the data will be utilized by $host_B$ 83, see blocks 130 and 56. Otherwise, a security protocol may be initiated to notify a network official of a potential security problem, see block 128.

### Proposed Protocol Modifications

This section describes proposed changes to protocols to utilize the above described method. For example, 3 authentication modes are illustrated in FIGS. 1, 3 and 4. Other authentication modes are possible with this scheme. One is the degenerate case of no authentication and two actually provide some authentication. The existence of the no authentication case permits hosts or networks not interested in the offered security properties to go without them and not have to pay for what they do not seek to use. The first real authentication mode suggested would use the MD5 digital signature algorithm applied across the header of the network-layer frame and then encoded using previously agreed upon DES encryption key using the chained block mode of DES. See, Rivest, R. & Dusse, S., "The MD5 Message-Digest Algorithm," RFC-1321, DDN Network Information Center (April, 1992); NBS, FIPS PUB 46, "Data Encryption Standard (DES)," National Bureau of Standards, U.S. Department of Commerce (January, 1977). The second real authentication mode would use the MD5 digest algorithm having been applied across the entire network-layer frame (exclusive of the authentication information field) and then have that encoded using RSA encryption.

### Additional Benefits

Another critical service that needs authentication is the network name service. If an intruder may masquerade as the legitimate nameservice provider, he may cause denial-of-service attacks, may modify data in transit, and may make other attacks on users of the internetwork. If however, the nameservice were authenticated, these attacks would not be possible.

Additionally, this authentication architecture could be used to implement the Clark-Wilson commercial security policy over a network or internetwork. To support Clark-Wilson, authentication of users real identities is essential. In the approach suggested here, the hosts would be authenticated to each other and could provide user authentication keys or such keys could be placed in a central directory service with its responses being authenticated. Full protection from host masquerading and network traffic control policies could be easily enforced. Since the Clark-Wilson policy is more concerned with integrity than confidentiality, this might be sufficient for a commercial firm or educational institution. Confidentiality could easily be added at the transport layer or above if it were needed and need not degrade performance for applications or users that didn't need it.

With a few extensions the approach outlined here could also support a multi-level security policy using either a "pink architecture" or a "red/black architecture". "Pink architecture" and "red/black architecture" are described in Cole, Raymond, Jr. et al., "Multilevel Secure Mixed-Media Communication Networks," Proceedings of the 1989 IEEE Conference on Military Communications (MILCOM '89), IEEE, New York, N.Y. For example, there might be encryption of user data immediately above the transport layer or the transport layer itself might be encrypted. Either asymmetric or symmetric keys could be used, though use of the latter would complicate key management. Because the network layer is fully authenticated, the receiving host may be

confident of where the transmission originated. Also, vulnerability to certain kinds of denial or service attacks may be significantly reduced by precluding the attacks described earlier. Use of the link encryption below the network layer to minimize the effectiveness of traffic analysis remains feasible and is unaffected by network layer or higher mechanisms such as these.

It appears feasible to implement the required changes to the existing protocols in a way that would remain interoperability with older versions. Moreover, this architecture scales nicely to large internetworks such as the current Internet. There are a number of hardware implementations of DES available already and it is feasible to implement digital signature algorithms and asymmetric key cryptography in hardware as well. If these were integrated into a chipset, the cost of authentication would be minimized. Moreover, hosts that do not wish to use authentication do not have to. Only the root nameservers and hosts wishing to use authentication services need pay for its implementation costs and overhead.

Although the present invention has been fully described in connection with the preferred embodiment thereof with reference to the accompanying drawings, it is to be noted that various changes and modifications are apparent to those skilled in the art. Such changes and modifications are to be understood, as included within the scope of the present invention as defined by the appended claims, unless they depart therefrom.

What is claimed is:

1. A method for authenticating an originating host at a receiving host, said method comprising the steps of:

(a) obtaining a network address and a public key of said receiving host;

(b) utilizing said public key from said receiving host in combination with a private key from said sending host to generate a cryptographic signature;

(c) transmitting said cryptographic signature along with data through a first subnetwork in at least one packet;

(d) receiving said at least one packet at said receiving host; and

(e) said receiving host utilizing a private key of said receiving host and a public key of said originating host to verify said cryptographic signature.

2. The method recited in claim 1 wherein an asymmetric algorithm is used to generate said cryptographic signature.

3. The method recited in claim 2 wherein said asymmetric algorithm is an RSA digital signature algorithm.

4. A method for authentication of an originating host at a receiving host site and one or more intermediate routers, said method comprising the steps of:

(a) obtaining a network address for said receiving host;

(b) utilizing a private key from said originating host to generate a cryptographic signature;

(c) transmitting said cryptographic signature along with data through a first subnetwork in at least one packet, having a first packet size;

(d) receiving said at least one packet at said receiving host; and

(e) said receiving host utilizing a public key of said originating host to verify said cryptographic signature.

5. The method recited in claim 4 wherein said packets are authenticated at an intermediate router by utilizing a public key of said originating host to verify said cryptographic signature.

6. The method recited in claim 4 wherein an asymmetric algorithm is used to generate said cryptographic signature.

7. The method recited in claim 6 wherein said asymmetric algorithm is an RSA digital signature algorithm.

8. A method for authentication of an originating host at a receiving host site and one or more intermediate routers, said method comprising the steps of:

(a) obtaining a network address for said receiving host;

(b) utilizing a private key from said originating host to generate a cryptographic signature;

(c) transmitting said cryptographic signature along with data through two or more subnetworks in at least one packet having a first packet size, where the packet is fragmented into 2 or more packet fragments during transit from said originating host to said receiving host;

(d) receiving said at least one packet at said receiving host; and

(e) said receiving host utilizing a public key of said originating host to verify said cryptographic signature.

9. The method recited in claim 8 wherein said transmitting step is conducted by transmitting a first fragmented packet of said first subnetwork packets to a first available intermediate router, and each subsequent fragmented packet of said first subnetwork packets following the progress of said first fragmented packet through said second subnetwork in a train like fashion.

10. The method recited in claim 4, wherein said at least one packet having a first packet size is fragmented and thereby forming at least two fragmented packet, said fragmented packets having a first fragmented packet which is transmitted to a first available intermediate router in said first subnetwork, and each subsequent fragmented packet following the progress of said first fragmented packet through said first subnetwork in a train like fashion.

11. The method recited in claim 9 wherein said packet fragments are authenticated at an intermediate router by first assembling said packet fragments and then utilizing a public key of said originating host to verify said cryptographic signature.

12. The method recited in claim 10 wherein said packet fragments are authenticated at an intermediate router by first assembling said packet fragments and then utilizing a public key of said originating host to verify said cryptographic signature.

13. The method recited in claim 1 wherein said receiving host, utilizing a public key of said originating host, verifies that said data has been sent by said sending host by utilizing said cryptographic signature.

14. The method recited in claim 4 wherein said receiving host, utilizing a public key of said originating host, verifies that said data has been sent by said originating host by utilizing said cryptographic signature.

* * * * *

US005511122A

United States Patent [19]

Atkinson

[11] Patent Number: 5,511,122

[45] Date of Patent: Apr. 23, 1996

[54] INTERMEDIATE NETWORK AUTHENTICATION

[75] Inventor: Randall Atkinson, Annandale, Va.

[73] Assignee: The United States of America as represented by the Secretary of the Navy, Washington, D.C.

[21] Appl. No.: 254,087

[22] Filed: Jun. 3, 1994

[51] Int. Cl.[6] ..... H04K 1/00

[52] U.S. Cl. ..... 380/25; 380/23; 380/21; 380/30

[58] Field of Search ..... 380/23, 25, 30, 380/4, 49, 21

[56] References Cited

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 4,438,824 | 3/1984 | Mueller-Schloer | 380/23 |
| 4,965,827 | 10/1990 | McDonald . | |
| 5,175,765 | 12/1992 | Perlman . | |
| 5,204,901 | 4/1993 | Hershey et al. . | |
| 5,204,961 | 4/1993 | Barlow . | |
| 5,241,599 | 8/1993 | Bellovin et al. . | |
| 5,280,583 | 1/1994 | Nakayama et al. | 395/200 |
| 5,371,794 | 12/1994 | Diffie et al. | 380/21 |
| 5,416,842 | 5/1995 | Aziz | 380/30 |

OTHER PUBLICATIONS

Tsudik, Gene, "*Datagram Authentication in Internet Gateways: Implications of Fragmentation and Dynamic Routing*", IEEE Journal on Selected Areas in Communications, vol. 7, No. 4, (May, 1989), IEEE, NY, NY.

ISI, Transmission Control Protocol, RFC–793 Network Information Center, (Sep., 1981).

Voydock, V. L. and Kent, S. T., "*Security in High-Level Network Protocols*", IEEE Communications, vol. 23, No. 7 (Jul., 1985).

Rivest, R. & Dusse, S., "*The MD5 Message–Digest Algorithm*," RFC–1321, DDN Network Information Center (Apr., 1992).

Cole, Raymond, Jr. et al., "*Multilevel Secure Mixed–Media Communication Networks*," Proceedings of the 1989 IEEE Conference on Military Communications (MILCOM '89), IEEE, N.Y., N.Y.

Clark, D.D. and Wilson, "*A Comparison of Commercial and Military Computer Security Policies*," Proceedings of the 1987 IEEE Symposium on Security & Privacy, IEEE Computer Society, Oakland, California (1987).

NBS, FIPS PUB 46, "*Data Encryption Standard (DES)*," National Bureau of Standards, U.S. Department of Commerce (Jan., 1977).

Schneier, B., "*Applied Cryptography*," John Wiley & Sons, Inc., NY, NY (1994), p. 3.

Bellovin, Steven M., "Security Problems in the TCP/IP Protocol Suite" ACM, Computer Communications Review, vol. 19, No. 2 (Apr., 1989), pp. 32–48.

Bellovin, Steven M., "*Limitations of the Kerberos Authentication System*", Proceedings of the Winter 1991 Usenix Conference, Usenix Association, Berkley, CA (1991).

Kent, S. T. & Linn, J., Privacy Enhancement for Internet Electronic Mail: Part II–Certificate–based Key Management, RFC–1114, DDN Network Information Center (Aug., 1989).

Kent, S. T. US DoD Security Options for the Internet Protocol, RFC–1108, DDN Network Information Cen

(List continued on next page.)

*Primary Examiner*—David C. Cain

*Attorney, Agent, or Firm*—Thomas E. McDonnell; Daniel Kalish

[57] ABSTRACT

An internetwork authentication method is provided for verifying a sending host by a receiving host or an intermediate router or gateway. The method comprises the steps of: obtaining a network address and a public key of a receiving host; utilizing the public key from the receiving host in combination with a private key of the originating host to generate a cryptographic signature; transmitting the signature along with data through a first subnetwork in at least one packet; receiving at least one packet at the receiving host; and the receiving host utilizing a private key of said receiving host site and a public key of said originating host to verify said cryptographic signature.

14 Claims, 4 Drawing Sheets

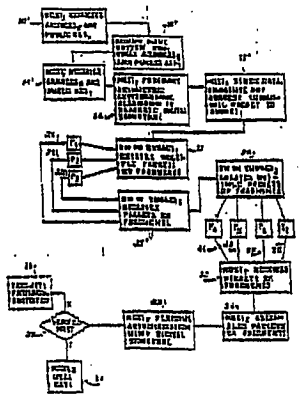


EXHIBIT E

OTHER PUBLICATIONS

ter (Nov., 1991).

Mockapetris, Paul, Domain Names–Implementation and Specification, RFC–1035, DDN Network Information Center (Nov., 1987).

Needham, R. M. and Schroeder, M. D., "*Using Encryption for Authentication in Large Networks of Computers*", Communications of the ACM, vol. 21, No. 12 (Dec., 1978).

"*Security Requirements for Cryptographic Modules*", Federal Information Processing Standards Publication 140–1, (Jan. 11, 1994), pp. 1–53.

Branstad, Dennis et al., "*SP4: A Transport Encapsulation Security Protocol*", Proceedings of 1987 NCSC Conference, pp. 158–161.

Nelson, Ruth, "*SDNS Services and Architecture*", Proceedings of 1987 NCSC Conference, pp. 153–157.

Lambert, Paul A., "*Layer Wars: Protect the Internet with Network Layer Security*", Motorola, Inc., Secure Telecommunications.

Dinkel, Charles (Editor), "*Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols*", U.S. Dept. of Commerce, Nat'l. Inst. Stds., NISTIR 90–4250.

# UNITED STATES DISTRICT COURT
# CENTRAL DISTRICT OF CALIFORNIA

## NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Mariana P. Pfaelzer and the assigned discovery Magistrate Judge is Fernando M. Olguin.

The case number on all documents filed with the Court should read as follows:

**SACV09- 376 MRP (FMOx)**

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

The United States District Judge assigned to this case will review all filed discovery motions and thereafter, on a case-by-case or motion-by-motion basis, may refer discovery related motions to the Magistrate Judge for hearing and determination

---

**NOTICE TO COUNSEL**

*A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).*

Subsequent documents must be filed at the following location:

[ ] **Western Division**
**312 N. Spring St., Rm. G-8**
**Los Angeles, CA 90012**

[X] **Southern Division**
**411 West Fourth St., Rm. 1-053**
**Santa Ana, CA 92701-4516**

[ ] **Eastern Division**
**3470 Twelfth St., Rm. 134**
**Riverside, CA 92501**

Failure to file at the proper location will result in your documents being returned to you.

Peter R. Afrasiabi (Bar No. 193336)
Christopher W. Arledge (Bar No. 200767)
Turner Green Afrasiabi & Arledge LLP
535 Anton Blvd., Ste. 850, Costa Mesa, CA 92626

**UNITED STATES DISTRICT COURT**
**CENTRAL DISTRICT OF CALIFORNIA**

| | |
|---|---|
| Network Signatures, Inc.,<br><br>PLAINTIFF(S)<br>v.<br>Fidelity Investments Institutional Services Company, Inc., a Massachusetts corporation,<br><br>DEFENDANT(S). | CASE NUMBER<br><br>**SACV09 -376 MRP (FMOx)**<br><br>**SUMMONS** |

TO: THE ABOVE-NAMED DEFENDANT(S):

YOU ARE HEREBY SUMMONED and required to file with this court and serve upon plaintiff's attorney Peter R. Afrasiabi, whose address is:

Turner Green Afrasiabi & Arledge LLP
535 Anton Blvd., Ste. 850, Costa Mesa, CA 92626

an answer to the ☒ complaint ☐ _____ amended complaint ☐ counterclaim ☐ cross-claim which is herewith served upon you within 20 days after service of this Summons upon you, exclusive of the day of service. If you fail to do so, judgement by default will be taken against you for the relief demanded in the complaint.

Clerk, U.S. District Court

Dated: 26 MAR 2009

By: DONNIE CARRIANTOS
Deputy Clerk

*(Seal of the Court)*

# UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA

## CIVIL COVER SHEET

**I (a) PLAINTIFFS** (Check box if you are representing yourself ☐)
Network Signatures, Inc.

**DEFENDANTS**
Fidelity Investments Institutional Services Company, Inc., a Massachusetts corporation

**(b)** County of Residence of First Listed Plaintiff (Except in U.S. Plaintiff Cases):
Orange County

County of Residence of First Listed Defendant (In U.S. Plaintiff Cases Only):
Suffolk County

**(c)** Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.)
Peter R. Afrasiabi (Bar No. 193336)
Christopher W. Arledge (Bar No. 200767)
Turner Green Afrasiabi & Arledge, LLP
535 Anton Blvd., Ste. 850, Costa Mesa, CA 92626 (714) 434-8750

Attorneys (If Known)

**II. BASIS OF JURISDICTION** (Place an X in one box only.)

☐ 1 U.S. Government Plaintiff
☐ 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** - For Diversity Cases Only
(Place an X in one box for plaintiff and one for defendant.)

| | 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. ORIGIN** (Place an X in one box only.)

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify): ☐ 6 Multi-District Litigation ☐ 7 Appeal to District Judge from Magistrate Judge

**V. REQUESTED IN COMPLAINT:** **JURY DEMAND:** ☑ Yes ☐ No (Check 'Yes' only if demanded in complaint.)

**CLASS ACTION under F.R.C.P. 23:** ☐ Yes ☑ No ☑ **MONEY DEMANDED IN COMPLAINT: $** Proven at trial

**VI. CAUSE OF ACTION** (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)
Patent Infringement, Permanent Injunction and Damages

**VII. NATURE OF SUIT (Place an X in one box only.)**

**OTHER STATUTES**
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce/ICC Rates/etc.
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit
☐ 490 Cable/Sat TV
☐ 810 Selective Service
☐ 850 Securities/Commodities /Exchange
☐ 875 Customer Challenge 12 USC 3410
☐ 890 Other Statutory Actions
☐ 891 Agricultural Act
☐ 892 Economic Stabilization Act
☐ 893 Environmental Matters
☐ 894 Energy Allocation Act
☐ 895 Freedom of Info. Act
☐ 900 Appeal of Fee Determination Under Equal Access to Justice
☐ 950 Constitutionality of State Statutes

**CONTRACT**
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loan (Excl. Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

**REAL PROPERTY**
☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

**TORTS PERSONAL INJURY**
☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Fed. Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☐ 360 Other Personal Injury
☐ 362 Personal Injury-Med Malpractice
☐ 365 Personal Injury-Product Liability
☐ 368 Asbestos Personal Injury Product Liability

**TORTS PERSONAL PROPERTY**
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

**BANKRUPTCY**
☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

**CIVIL RIGHTS**
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/Accommodations
☐ 444 Welfare
☐ 445 American with Disabilities - Employment
☐ 446 American with Disabilities - Other
☐ 440 Other Civil Rights

**PRISONER PETITIONS**
☐ 510 Motions to Vacate Sentence Habeas Corpus
☐ 530 General
☐ 535 Death Penalty
☐ 540 Mandamus/ Other
☐ 550 Civil Rights
☐ 555 Prison Condition

**FORFEITURE/ PENALTY**
☐ 610 Agriculture
☐ 620 Other Food & Drug
☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 630 Liquor Laws
☐ 640 R.R. & Truck
☐ 650 Airline Regs
☐ 660 Occupational Safety /Health
☐ 690 Other

**LABOR**
☐ 710 Fair Labor Standards Act
☐ 720 Labor/Mgmt. Relations
☐ 730 Labor/Mgmt. Reporting & Disclosure Act
☐ 740 Railway Labor Act
☐ 790 Other Labor Litigation
☐ 791 Empl. Ret. Inc. Security Act

**PROPERTY RIGHTS**
☐ 820 Copyrights
☑ 830 Patent
☐ 840 Trademark

**SOCIAL SECURITY**
☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

**FEDERAL TAX SUITS**
☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS-Third Party 26 USC 7609

**VIII(a). IDENTICAL CASES:** Has this action been previously filed and dismissed, remanded or closed? ☑ No ☐ Yes

If yes, list case number(s): **SACV09 -376 MRP (FMOx)**

**FOR OFFICE USE ONLY:** Case Number: _____

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

**VIII(b). RELATED CASES:** Have any cases been previously filed that are related to the present case? ☐ No ☑ Yes

If yes, list case number(s): See Attachment A

**Civil cases are deemed related if a previously filed case and the present case:**

(Check all boxes that apply)
- ☐ A. Arise from the same or closely related transactions, happenings, or events; or
- ☑ B. Call for determination of the same or substantially related or similar questions of law and fact; or
- ☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
- ☑ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

**IX. VENUE:** List the California County, or State if other than California, in which **EACH** named plaintiff resides (Use an additional sheet if necessary)

☐ Check here if the U.S. government, its agencies or employees is a named plaintiff.
Network Signatures, Inc. - Orange County

List the California County, or State if other than California, in which **EACH** named defendant resides. (Use an additional sheet if necessary).

☐ Check here if the U.S. government, its agencies or employees is a named defendant.
Fidelity Investments Institutional Services Company, Inc. - Massachusetts

**List the California County**, or State if other than California, in which **EACH** claim arose. (Use an additional sheet if necessary)
**Note:** In land condemnation cases, use the location of the tract of land involved.
Orange County

**X. SIGNATURE OF ATTORNEY (OR PRO PER):** _____ **Date** 3/24/09

**Notice to Counsel/Parties:** The CV-71 (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. This form, approved by the Judicial Conference of the United States in September ~~1974~~ is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

| Nature of Suit Code | Abbreviation | Substantive Statement of Cause of Action |
|---|---|---|
| 861 | HIA | All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b)) |
| 862 | BL | All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923) |
| 863 | DIWC | All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g)) |
| 863 | DIWW | All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g)) |
| 864 | SSID | All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended. |
| 865 | RSI | All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g)) |

**ATTACHMENT A**

SACV 06-629 JVS, SACV 07-1429 JVS, SACV 07-1430 JVS, SACV 07-1427 JVS, SACV 08-00775 JVS, SACV 08-00776 JVS, SACV 08-00777 JVS, SACV 08-00778 JVS, SACV 08-00779 JVS, SACV 09-197 JVS, SACV 09-206 JVS, SACV 09-196 JVS SACV 07-1426 AHS, SACV 08-00718 DOC, SACV 06429 SJO