PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 89441

OR

□ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 89441

OR

□ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Research In Motion Limited
295 Phillip Street
Waterloo, Ontario, Canada N2L 3W8

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	Oct 8/09
Name	Jim Balsillie	Telephone	519-888-7465
Title	Co-Ceo		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Neil P. Adams, et al.

Application No./Patent No.: 11/065,901 Filed/Issue Date: February 25, 2005

Titled: System and Method for Configuring Devices for Secure Operations

Research In Motion Limited, a Corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. □ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is ________ %); or

3. □ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 016864, Frame 0265, or for which a copy therefore is attached.

OR

B. □ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: ________ To: ________
The document was recorded in the United States Patent and Trademark Office at
Reel ________, Frame ________, or for which a copy thereof is attached.

2. From: ________ To: ________
The document was recorded in the United States Patent and Trademark Office at
Reel ________, Frame ________, or for which a copy thereof is attached.

3. From: ________ To: ________
The document was recorded in the United States Patent and Trademark Office at
Reel ________, Frame ________, or for which a copy thereof is attached.

□ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Matthew W. Johnson/ July 14, 2011
Signature Date

Matthew W. Johnson Attorney (Agent)
Printed or Typed Name Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	
	Filing Date	
	First Named Inventor	Neil P. Adams
	Art Unit	
	Examiner Name	
	Attorney Docket Number	555255-013133

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5935248		1999-08-00	Kuroda, Yasutsugu	
	2	6202157		2001-03-13	Brownlie et al	
	3	6732168		2004-05-04	Bearden et al	
	4	6775536		2004-08-00	Geiger et al	
	5	7131003		2006-10-00	Lord et al	
	6	7317699		2008-01-00	Godfrey et al	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	
Filing Date	
First Named Inventor	Neil P. Adams
Art Unit	
Examiner Name	
Attorney Docket Number	555255-013133

	1	20020165912		2002-11-00	Wenocur et al	
	2	20020186845		2002-12-00	Dutta et al	
	3	20030204722		2003-10-00	Schoen et al	
	4	20040019807		2004-01-00	Freund, Gregor P.	
	5	20050183138		2005-08-00	Phillips et al	
	6	20050190764		2005-09-00	Shell et al	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number^3	Country Code^2 j	Kind Code^4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T^5
	1	0069120	WO	A1	2000-11-16			□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T^5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		
	Filing Date		
	First Named Inventor	Neil P. Adams	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	555255-013133	

	1	Sems, Marty, "Verifying Identity in a Digital World", August 2000.	□
	2	S. Gavrila, et al., "Assigning and Enforcing Security Policies on Handheld Devices", Canadian Information Technology Security Symposium, May 17, 2002, Pages 0-7, XP002440113.	□
	3	International Search Report of Application No. PCT/CA2005/000294, date of mailing June 20, 2005, 11 pages.	□
	4	Supplementary European Search Report, Issued July 11, 2007 by European Patent Office, for European Patent Application No. 05714536.	□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		
	Filing Date		
	First Named Inventor	Neil P. Adams	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	555255-013133	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

□ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew W. Johnson/	Date (YYYY-MM-DD)	2011-07-14
Name/Print	Matthew W. Johnson	Registration Number	59,108

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

WO0069120

Publication Title:

MANAGING MULTIPLE NETWORK SECURITY DEVICES FROM A MANAGER DEVICE

Abstract:

The present invention is directed to a facility for using a security policy manager device to remotely manage multiple network security devices (NSDs). The manager device can also use one or more intermediate supervisor devices to assit in the management. Security for the communication of information between various devices can be provided in a variety of ways. The system allows the manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information. For example, the manager device can distribute the template to multiple NSDs by sending a single copy of the template to a supervisor device associated with the NSDs and by then having the supervisor device update each of the NSDs with a copy of the template.; Other information useful for implementing security policies can also be distributed to the NSDs in a similar manner. The system also allows a manager device to retrieve, analyze and display all of the network security information gathered by the various NSDs while implementing security policies. Each NSD can forward its network security information to a supervisor device currently associated with the NSD, and the manager device can retrieve network security information of interest from the one or more supervisor devices which store portions of the information and then aggregate the retrieved information in an appropriate manner.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 12/24, 29/06	A1	(11) International Publication Number: WO 00/69120 (43) International Publication Date: 16 November 2000 (16.11.00)

(21) International Application Number: PCT/US00/09942

(22) International Filing Date: 13 April 2000 (13.04.00)

(30) Priority Data:
09/307,332 6 May 1999 (06.05.99) US

(71) Applicant *(for all designated States except US)*: WATCHGUARD TECHNOLOGIES, INC. [US/US]; Suite 200, 316 Occidental Avenue South, Seattle, WA 98104 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ROTHERMEL, Peter, M. [US/US]; 3635 175th Court N.E., Redmond, WA 98052 (US). BONN, David, Wayne [US/US]; 12324 5th Place West, Everett, WA 98204 (US). MARVAIS, Nick, T. [US/US]; 18524 Linden Avenue N., Apartment 306, Shoreline, WA 98133 (US).

(74) Agents: WHITE, James, A., D. et al.; Perkins Coie LLP, 1201 Third Avenue, Suite 4800, Seattle, WA 98101–3099 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: MANAGING MULTIPLE NETWORK SECURITY DEVICES FROM A MANAGER DEVICE

(57) Abstract

The present invention is directed to a facility for using a security policy manager device to remotely manage multiple network security devices (NSDs). The manager device can also use one or more intermediate supervisor devices to assit in the management. Security for the communication of information between various devices can be provided in a variety of ways. The system allows the manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD–specific information. For example, the manager device can distribute the template to multiple NSDs by sending a single copy of the template to a supervisor device associated with the NSDs and by then having the supervisor device update each of the NSDs with a copy of the template. Other information useful for implementing security policies can also be distributed to the NSDs in a similar manner. The system also allows a manager device to retrieve, analyze and display all of the network security information gathered by the various NSDs while implementing security policies. Each NSD can forward its network security information to a supervisor device currently associated with the NSD, and the manager device can retrieve network security information of interest from the one or more supervisor devices which store portions of the information and then aggregate the retrieved information in an appropriate manner.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

MANAGING MULTIPLE NETWORK SECURITY DEVICES FROM A MANAGER DEVICE

TECHNICAL FIELD

The present invention relates generally to communicating information between computers, and more particularly to using a manager device to remotely manage multiple network security devices.

BACKGROUND OF THE INVENTION

As computer systems and other network devices (*e.g.*, printers, modems, and scanners) have become increasingly interconnected, it is increasingly important to protect sensitive information (*e.g.*, confidential business data, access information such as passwords, or any type of data stored on certain devices) stored on one network device from unauthorized retrieval by other network devices. The prevalence of the Internet and the growth of the World Wide Web have only exacerbated this issue.

One way to address this issue involves the use of network security devices ("NSDs") which attempt to control the spread of sensitive information so that only authorized users or devices can retrieve such information. Some types of NSDs, such as firewalls and security appliances, have a group of one or more trusted network devices (or networks consisting of trusted network devices) which the NSD attempts to protect from unauthorized external access. These NSDs monitor network information passing between external network devices and the devices in their group of trusted or internal devices. In addition, these NSDs typically implement a specified security policy by preventing the passage of unauthorized network information between the external and the trusted devices.

Those skilled in the art will appreciate that network information can be transmitted in a variety of formats. For example, network information is often transmitted as a series of individual packets of information, such as TCP/IP (Transfer Control Protocol/Internet Protocol) packets. While such packets will typically include the network address (*e.g.*, IP address) of the device to receive the information, other data about the network information (*e.g.*, the specific type of information being requested or sent) may be difficult to ascertain.

While a properly configured NSD can protect information stored on or accessible from trusted devices, it can be difficult to configure NSDs so that they correctly implement the desired security policies. One source of difficulty in configuring NSDs arises from the large number of types of network information which may be encountered. For example, there are a large number of network services and protocols which external devices may attempt to provide to trusted devices or access from trusted devices.

Such network services and protocols include, but are not limited to, Archie, auth (ident), DCE-RPC (Distributed Computing Environment Remote Procedure Call), DHCP (Dynamic Host Configuration Protocol) Client and Server, DNS (Domain Name Service), finger, FTP (File Transfer Protocol), gopher, H.323, HTTP (HyperText Transfer Protocol), Filtered-HTTP, Proxied-HTTP, ICMP (Internet Control Message Protocol), NNTP (Network News Transfer Protocol), NTP (Network Time Protocol), ping, POP (Post Office Protocol) 2 and 3, RealNetworks, rlogin, rsh (Remote SHell), SMB (Simple Block Messaging), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), syslog, ssh (Secure SHell), StreamWorks, TCP/IP, telnet, Time, traceroute, UDP (User Datagram Protocol), VDOLive, WAIS (Wide Area Information Services), whois, and other device-specific services. Those skilled in the art will appreciate the uses and details of these services and protocols, including the device ports typically used with the services and protocols and the specified format for such information (*e.g.*, the TCP/IP packet definition).

Another source of difficulty in configuring NSDs arises from the variety of ways to handle network information of different types. For example, for each type of service or protocol, a NSD may wish to take different actions for (*e.g.*, allow passage of, deny passage of, or otherwise manipulate) the corresponding network information of that service or protocol. The decision to take these different actions can also be based on additional factors such as the direction of information flow (*i.e.*, whether the network information is passing from a trusted device or to a trusted device) or on the basis of the sender or the intended recipient of the information (*e.g.*, whether the network information is passing from or to specific network devices or is passing from or to any network device of a specified class, such as any external device).

The types of actions to be taken for the monitored network information (based on the various factors such as the services and protocols being used, the direction of the information flow, and the classes of devices of the sender and the intended recipient) provide an initial incomplete security policy. Various device-specific information is necessary to configure a particular NSD with a specific security policy that can be implemented by the device. The device-specific information which must typically be specified to create a specific security policy includes, for example, the network address of the NSD and the network addresses of some or all of the trusted devices. If a particular network service is to be provided to external devices by a trusted device, such as FTP access, information about the trusted FTP server must also be available to the NSD.

A user such as a system administrator typically defines the specific security policy for a NSD by determining the services and protocols of interest and then configuring the NSD to protect the trusted devices as appropriate. However, configuring an NSD can be time-consuming, and any mistakes in the configuration (*e.g.*, failure to define how a particular service should be handled, or allowing default behaviors to allow passage of network information) can compromise the ability of the NSD to protect sensitive information. Thus, the need for system administrators to configure each NSD can cause various problems.

When it is necessary to configure large numbers of NSDs, such problems are only exacerbated. If the security policies across some or all of the NSDs should be consistent (*e.g.*, multiple devices in use by a single company), the likelihood of mistakes increases. If the system administrator merely copies the specific security policy from one NSD to another, mistakes may occur in re-specifying the various NSD-specific configuration information. Alternately, if the system administrator attempts to re-create the general security policy independently on each NSD, various mistakes may occur such as neglecting to configure a type of service or incorrectly configuring the actions for such a type.

In addition to implementing security policies which may restrict the passage of some network information, NSDs typically gather network security information about events of interest, including encountering types of network information that is encountered as well as various actions taken by the NSD. The network security information can be displayed to users such as system administrators so that they can verify that the security policy is correctly implemented, produce reports about the types and quantities of network information that is allowed to pass and that is blocked from passage, and identify when external activities of concern (*e.g.*, a hacker attack on the NSD) are occurring. NSDs typically maintain a local storage, often referred to as a log, of the security information that they gather.

Some NSDs include computer software components executing on general-purpose or dedicated computer hardware. For such an NSD, the executing software components assist in implementing the specific security policies defined for the NSD. Use of software components allows the operation of the NSD to be upgraded in an efficient manner by replacing some or all of the existing software components with new software components. Such new software is typically distributed via physical media such as CDs or optical disks, and is loaded onto the NSD by an individual such as a system administrator.

SUMMARY OF THE INVENTION

Some embodiments of the present invention provide a facility for using a security policy manager device to remotely manage multiple network security devices (NSDs). In some embodiments, the manager device uses one or more intermediate supervisor devices to assist in the management. Security for the communications between the manager device, supervisor devices, and NSDs can be provided in a variety of ways.

The facility allows the manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information. For example, the manager device can distribute the template to multiple NSDs by sending a single copy of the template to a supervisor device associated with the NSDs and by then having the supervisor device update each of the NSDs with a copy of the template. Other information useful for implementing security policies for the NSDs, such as software components to be executed by the NSDs, can also be distributed by the manager device to the NSDs in a similar manner.

The facility also allows a manager device to retrieve, analyze and display the network security information gathered by the various NSDs while implementing security policies. Each NSD can forward its network security information to a supervisor device currently associated with the NSD, and can switch supervisor devices if the current supervisor device becomes unavailable. When the manager device desires the network security information for an NSD, the manager device contacts the one or more supervisor devices which store portions of the network security information of interest, retrieves the various portions of the network security information, and then aggregates the retrieved information in an appropriate manner.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating an embodiment of the Network Security Device Management (NSDM) system of the present invention.

Figure 2 is a block diagram illustrating the flow of network security information from a network security device (NSD) to the manager device.

Figures 3A-3H are examples of security policy templates.

Figures 4A-4H are an example of network security information generated by implementing a specific security policy.

Figures 5A-5D are examples of a manager device's hierarchical view of multiple supervisor devices and NSDs and of corresponding configuration and network information.

Figure 6 is an example of one or more NSD software components which can be distributed by a manager device.

Figure 7 is an exemplary flow diagram of an embodiment of the Network Security Device routine.

Figure 8 is an exemplary flow diagram of an embodiment of the Filter Network Packets subroutine.

Figure 9 is an exemplary flow diagram of an embodiment of the Generate Network Security Information subroutine.

Figure 10 is an exemplary flow diagram of an embodiment of the Respond To Management Message subroutine.

Figure 11 is an exemplary flow diagram of an embodiment of the Supervisor Device routine.

Figure 12 is an exemplary flow diagram of an embodiment of the Process NSD Message subroutine.

Figure 13 is an exemplary flow diagram of an embodiment of the Process Manager Or Supervisor Device Message subroutine.

Figures 14A and 14B are exemplary flow diagrams of an embodiment of the Manager Device routine.

DETAILED DESCRIPTION OF THE INVENTION

An embodiment of the present invention provides a method and system for using a manager device to remotely manage multiple network security devices. In particular, the Network Security Device Management (NSDM) system allows a security policy manager device to create a consistent security policy for multiple network security devices (NSDs) by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information. Other information useful for implementing security policies for the NSDs, such as software components to be executed by the NSDs or lists of devices from whom information is to be blocked, can also be distributed by the manager device to the NSDs in a similar manner. The NSDM system also allows a manager device to retrieve, analyze and display the network security information gathered by the various NSDs while implementing security policies. In some embodiments, the manager device uses one or more intermediate supervisor devices to assist in managing the multiple NSDs.

Security policy templates can be defined by a user of the manager device and then used to implement consistent network security policies across multiple NSDs while reducing the risk of configuration error. Each template defines default network information filtering rules for various common services and protocols, and uses defined aliases to represent various specific devices of interest for a particular NSD. Security policy templates are discussed in greater detail below, as well as in the co-pending U.S. Patent Application entitled "GENERALIZED NETWORK SECURITY POLICY TEMPLATES FOR IMPLEMENTING SIMILAR NETWORK SECURITY POLICIES ACROSS MULTIPLE NETWORKS," filed May 6, 1999, incorporated herein by reference.

In order to remotely manage multiple NSDs, a manager device can use one or more intermediate supervisor devices. For example, after a security policy template is defined, the manager device can distribute the template to multiple NSDs by sending a single copy of the template to a supervisor device associated with the NSDs and by then having the supervisor device update each of the NSDs with a copy of the template. Each of the NSD template copies can then be configured with NSD-specific information from one or more of a variety of sources, such as by the manager device, by a local user such as a system administrator, or automatically such as with DNS information. In particular, aliases in the template copy on a particular NSD can be replaced with information about the specific corresponding devices that are protected by the NSD, and NSD-specific access information can also be specified. For example, an alias for an HTTP server can be replaced with the specific network address and name of the actual HTTP server.

Other information useful for implementing security policies for the NSDs, such as software components to be executed by the NSDs, lists of devices to be blocked (*i.e.*, to block information flowing from and/or to the device), or updates to existing templates in use, can also be distributed by the manager device to the NSDs in a similar manner via the supervisor devices. Such information can also be configured with NSD-specific information if necessary in the manner described above. Those skilled in the art will appreciate that configuration of an NSD can occur not only when the NSD is initially installed, but also at later times. In addition to providing information to the NSDs, the manager device can also provide various types of information to the supervisor devices (*e.g.*, software updates for software executing on the supervisor devices).

One or more intermediate supervisor devices can also assist the manager device in retrieving, analyzing and displaying the network security information gathered by the various NSDs. As each NSD executes and implements its specific security policy, the NSD gathers network security information about its activities and about the network information that is monitored. Each NSD forwards its network security information to a host supervisor device currently associated with the NSD so that the supervisor device can host the network security information by storing and/or processing it. If the supervisor device currently associated with an NSD becomes unavailable, the NSD instead forwards its network security information to one or more alternate host supervisor devices. In this manner, even if one supervisor device becomes unavailable, the network security information for the NSDs that were associated with the supervisor device is not lost. When the manager device wants to retrieve the network security information for an NSD, the manager device contacts the one or more supervisor devices which store portions of the network security information of interest, retrieves the various portions of the network security information, and then aggregates the retrieved information in an appropriate manner.

In some embodiments, the manager device and supervisor devices are external devices. Security for the communications between the manager device, supervisor devices, and NSDs can be provided in a variety of ways. For example, any of the information transmitted between the NSDs and the supervisor devices and between the supervisor devices and the manager device can be protected from unauthorized access by encrypting the information (*e.g.*, using Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode). In addition, various schemes can be used to ensure that NSDs and supervisor devices provide information only to authorized devices or users, such as by using passwords, hashing passwords to produce keys, challenge/response, shared secrets, digital IDs, or a list of devices defined as being authorized to request and/or receive information. Part of the NSD-specific configuration of each NSD can include associating one or more supervisor devices authorized to communicate with the NSD, as well as providing specific information about how the communication is to occur. User authentication can be performed in a variety of ways, such as by using WINDOWS NT™ Domain Users and Groups RADIUS user authentication, or CRYPTOcard.

Referring now to Figure 1, an embodiment of the Network Security Device Management (NSDM) system 100 includes a security policy manager device 110 able to communicate with multiple supervisor devices 120 and 160, also referred to as host devices or event processors. Each supervisor device is associated with multiple NSDs, with supervisor device 120 associated with NSDs 130 through 140 and with supervisor device 160 associated with NSDs 161 through 162. Each NSD protects one or more trusted devices from external devices, such as NSDs 130 and 140 protecting devices (not shown) in internal networks 135 and 145 respectively from devices (not shown) in external network 190. For the sake of brevity, supervisor device 160 and NSDs 161 through 162 are not described in detail.

In some embodiments, additional classes of devices which the NSD will protect are defined, with different security policies defined for each class of devices. For example, internal devices which are in direct communication with external devices (*e.g.*, HTTP and FTP servers) may be specified in an optional class. Optional devices are typically afforded some level of trust greater than external devices but less than trusted devices, such as by monitoring some communications between optional and trusted devices. Thus, security policy templates and specific security policies can be viewed as defining levels of trust given to various specific devices or classes of devices.

Each NSD has a supervisor device which is designated as the primary supervisor device for that NSD. For example, supervisor device 120 is the primary supervisor for NSDs 130 through 140, and those NSDs store information about supervisor device 120 (*e.g.*, the device's network address) with their respective specific security policy information 133 and 143 on storage devices 131 and 141. In a similar manner, supervisor device 160 is the primary supervisor for NSDs 161 through 162. NSDs 130 and 140 also store any required access information (*e.g.*, one or more unique passwords which supervisor device 120 must provide in order to gain access to the NSDs) along with their respective device access information 134 and 144. The NSD-specific access information and primary supervisor device information can also optionally be stored by the manager device along with its supervisor device and NSD access information 115 and specific security policy information 116 respectively. Those skilled in the art will appreciate that storage devices 131 and 141 can be implemented in a variety of ways, such as by using local or remote storage, and by using a variety of storage media (*e.g.*, magnetic disk, flash RAM, etc.).

The manager device has one or more input/output devices 118 (such as a display) to enable a user (not shown) to interact with the manager device. The manager device also stores a variety of information on storage device 111, including one or more NSD software updates 112, security policy templates 113, and aggregated network security information 114 from one or more NSDs. The manager device also optionally stores supervisor device and NSD access information 115 (*e.g.*, passwords and a decryption key for stored information) as well as specific security policy information 116 (including NSD-specific configuration information) for one or more NSDs. Those skilled in the art will appreciate that storage device 111 can be implemented in a variety of ways, such as by using local or remote storage, and by using a variety of storage media (*e.g.*, magnetic disk, flash RAM, etc.).

When a user of the manager device desires to establish or modify a security policy for one or more NSDs such as NSDs 130 and 140, the user first selects one of the security policy templates 113 or creates a new security policy template. Security policy templates are discussed in greater detail below with respect to Figure 3. The manager device then determines the one or more primary supervisor devices for the NSDs of interest, such as by retrieving this information from its specific security policy information 116. If this information is not stored by the manager device, the manager device can obtain the information in a variety of ways, such as by querying the NSDs of interest or by querying the various known supervisor devices.

After the one or more primary supervisor devices are known, the manager device sends a single copy of the security policy template to each of the primary supervisor devices. For example, if the NSDs 130 and 140 are selected, a copy of the template is sent to supervisor device 120. The primary supervisor devices then send a copy of the security policy template to each of the selected NSDs. Each NSD stores its copy of the security policy template with the NSD's specific security information.

Each NSD's copy of the security policy template can then be configured with information specific to the NSD. For example, information about specific devices of interest from internal network 135 will be retrieved, and will be used to configure the security policy template for NSD 130. This NSD-specific information will be used to configure the security policy template into a specific security policy for the NSD, and the information will be stored with the specific security policy information for the NSD. The NSD-specific configuration can be conducted by a user via the manager device, by a local user such as a system administrator for the NSD, or automatically via a device-identifying service such as DNS.

When a user of the manager device desires to initially load or modify the software to be executed by one or more NSDs such as NSDs 130 and 140, the user first selects the software of interest, such as from NSD software updates information 112. The user can update some or all of the software components used by the NSDs. The manager device then distributes the software components to the NSDs in the same manner as for the security policy templates, including configuring the copies of the software with NSD-specific information if necessary. Each NSD stores the software, such as NSDs 130 and 140 storing their software with their security device software 132 and 142 respectively. The NSDs will implement the defined specific security policy by executing the software and using the stored specific security policy information. Those skilled in the art will appreciate that other types of information other than security policy templates and software can be distributed from the manager device to the NSDs in a similar manner.

As the NSDs execute their specific security policies, they gather various network security information of interest. Each NSD forwards its network security information to its primary supervisor device for storage. The network security information can be forwarded to the supervisor device in a variety of ways, such as immediately upon generation, on a periodic basis, or when the supervisor device requests the information. For example, NSDs 130 and 140 forward their network security information to supervisor device 120 for storage in the supervisor device's network security information log 125. If supervisor device 120 becomes unavailable, NSDs 130 and 140 will forward their network security information to another supervisor device, such as supervisor device 160. Supervisor device 160 stores the network security information it receives in network security information log 165. Thus, each supervisor device maintains one or more logs containing network security information sent by NSDs associated with the supervisor device.

When a user of the manager device desires to see the network security information of an NSD such as NSD 120, the manager device retrieves the network security information from each supervisor device which stores any of the network security information (*e.g.*, any security information generated between two specified times, or all security information that is available). The manager device can determine these one or more supervisor devices in a variety of ways. For example, each of the supervisor devices can periodically inform the manager device of the NSDs which are currently associated with the supervisor device, and the manager device can store this information with its specific security policy information 116. The manager device can then aggregate the network security information that is retrieved from multiple supervisor devices in a variety of ways, such as chronologically, by event type, etc. This aggregated network security information can be stored by the manager device in the aggregated network security information 114 of the manager device, either individually or with the security information of other NSDs.

Those skilled in the art will appreciate that each device of the NSDM system may be composed of various components such as a CPU, memory, input/output devices (*e.g.*, a display and a keyboard), and storage (*e.g.*, a hard disk or non-volatile flash RAM). In addition, those skilled in the art will appreciate that the described embodiment of the NSDM system is merely illustrative and is not intended to limit the scope of the present invention. The system may contain additional components or may lack some illustrated components. In particular, there may be multiple manager devices and/or multiple hierarchical layers of supervisor devices such that some supervisor devices supervise other supervisor devices. Alternately, the manager device and one or more supervisor devices may be implemented as a single computer system such that the manager device communicates directly with NSDs. Also, in some embodiments the devices which host network security information for the NSDs can be separate devices from those which supervise and send management information to the NSDs. Accordingly, the present invention may be practiced with other configurations.

Referring now to Figure 2, an embodiment of the NSDM system is used to illustrate how network security information from an NSD is stored by multiple supervisor devices. In some embodiments, each NSD has not only a primary supervisor device which is associated with the NSD, but also one or more additional associated supervisor devices (*e.g.*, secondary and tertiary devices, or multiple secondary devices). As with the primary supervisor device, these additional supervisor devices for an NSD can be specified in a variety of ways, such as by a user of the manager device during configuration of the NSD or automatically based on a variety of criteria (*e.g.*, geographic proximity to the NSD, capacity of the supervisor device, etc.). Each NSD can store information about the additional supervisor devices with their specific security policy information, as well as any required access information for the additional supervisor devices along with their device access information.

As is discussed above with respect to Figure 1, supervisor device 120 has been designated as the primary supervisor device for NSD 130. As is illustrated in Figure 2, two other supervisor devices have also been associated with NSD 130. In particular, supervisor device 160 has been designated as a secondary supervisor device for NSD 130, and supervisor device 210 has been designated as a tertiary supervisor device. Those skilled in the art will appreciate that any number of supervisor devices could be associated with any given NSD, and that different NSDs can have different groups of associated supervisor devices. Supervisor devices 160 and 210 maintain network security information logs 165 and 215 respectively, and supervisor devices 120, 160 and 210 are all able to communicate with security policy manager device 110.

As is illustrated, NSD 130 protects multiple trusted devices 220 through 230 in internal network 135 from external devices in external network 190 (not shown). As NSD 130 implements its specific security policy and notes events of interest, it gathers various network security information related to the events. When NSD 130 has network security information that is to be transmitted to a supervisor device for storage, NSD 130 first determines if primary supervisor device 120 is available to host the information (*e.g.*, by sending a status query message to the device). If primary supervisor device 120 is able to receive network security information from NSD 130 and has the capacity to store the information, NSD 130 sends the network security information to supervisor device 120 for storage in the network security information log 125.

If, however, primary supervisor device 120 is not available to host the network security information from NSD 130, the NSD determines an alternate host supervisor device (referred to as a "fail-over"). Since supervisor device 160 has been designated as the only secondary supervisor device, NSD 130 determines if that supervisor device is available to host the network security information. If so, supervisor device 160 becomes the supervisor device currently associated with NSD 130, and the NSD forwards the information to the supervisor device. If supervisor device 160 is not available, the NSD determines a next supervisor device (*e.g.*, supervisor device 210) to check for availability. In this manner, the network security information for a single NSD may be stored across multiple host supervisor devices. As discussed above, the manager device can be informed as to the NSDs currently associated with each supervisor device in a variety of ways, such as by the supervisor devices or the NSDs periodically sending status messages to the manager device.

The details of how the fail-over process works can be implemented in a variety of ways. For example, in some embodiments after NSD 130 has switched its current association to an alternate supervisor device such as supervisor device 160, NSD 130 will continue to use that supervisor device as its host device until that supervisor device becomes unavailable. Alternately, the NSD could instead continue to try to send network security information to its primary supervisor device even if the current supervisor device remains available, such as by periodically checking the availability of the primary supervisor device or by first attempting to send each portion of network security information to the primary supervisor device. In addition, if an alternate supervisor device such as supervisor device 160 becomes unavailable, NSD 130 could first check the primary supervisor device for availability before checking other alternate supervisor devices, or could instead check the next supervisor device (supervisor device 210) that is associated with the NSD.

Those skilled in the art will also appreciate that fail-over among multiple supervisor devices can occur in a variety of ways. For example, additional supervisor devices can be associated with an NSD only when needed, such as when the primary supervisor device becomes unavailable. In addition, the NSDs may use a currently associated host supervisor device for reasons other than storing network security information, such as for forwarding messages to the manager device or to other NSDs.

Figures 3A-3H are examples of security policy templates. Figure 3A is a conceptual diagram illustrating the generation from a single security policy template of specific security policies for each of several NSDs and their respective internal networks. A security template 300 is first generated, such as by a user of the manager device. Then, for each of a number of different networks 315, 325, 335, etc., the user generates a network profile containing NSD-specific information for implementation by the NSD protecting that network. These network profiles are shown as network profiles 310, 320, 330, etc. In order to generate the specific security policy for each network, the security policy template is combined with the network profile for that network. For example, in order to create security policy 315 for network 1, the security policy template 300 is combined with network profile 310 for network 1.

Figure 3B is a conceptual diagram illustrating the creation of a security policy in greater detail. In particular, Figure 3B shows the creation of security policy 315 for network 1 shown in Figure 3A. Figure 3B shows that the security policy template 300 contains a number of security policy filter rules, including security policy rule 301. Security policy rule 301 specifies that outgoing FTP connections are allowed only from network elements defined as being within the "InformationServices" alias. While only one security policy rule is shown in security policy template 300 to simplify this example, security policy templates often have a larger number of such security policy rules.

The network profile 310 for network 1 contains a definition of the "InformationServices" alias 311. It can be seen that this definition defines the "InformationServices" alias to include the network elements at the following IP addresses:

220.15.23.52
220.15.23.53
220.15.23.97

In general, a network profile contains an alias definition like alias definition 311 for each alias used in the security policy template.

When the security policy template 300 and the network profile 310 for network 1 are combined to create the security policy 315 for network 1, the facility replaces the "InformationServices" alias in rule 301 with the network addresses listed for the "InformationServices" alias in definition 311. Doing so produces rule 316 in the security policy 315 for network 1, which indicates that outgoing FTP connections are allowed only from the network elements having IP addresses 220.15.23.52, 220.15.23.53, and 220.15.23.97. In the same manner, for each additional rule in security policy template 300, each occurrence of an alias is replaced with the network addresses of the network elements defined to be within the alias in the network profile 310 for network 1. As a result, the rules in security policy 315 for network 1, which are to be implemented in network 1, specifically refer to network elements within network 1. In this sense, they differ from the rules in security policies 325 and 335, which specifically refer to network elements within networks 2 and 3, respectively.

Figures 3C-3H provide exemplary graphical user interface screens such as may be provided by a manager device to assist in defining security policy templates. Referring now to Figure 3C, a variety of aliases are available to be used in creating security policy templates. Note that aliases may be related to services and protocols (*e.g.*, H323 and FTP) as well as to conceptual identifications of one or more network devices such as may be based on a particular NSD customer's network (*e.g.*, Accounting, Marketing, Production, Sales, and TopMgmt). As is illustrated, filter rules have been defined for the H323 and FTP aliases. Referring now to Figure 3D, a specific filter rule such as for a particular service is illustrated in detail, allowing control for incoming and outgoing packets based on specific senders and recipients. Each filter rule can include associated information as to whether to generate network security information when the rule applies (*e.g.*, via the Logging button). Referring now to figure 3E, an interface for defining aliases is shown along with a list of various defined exemplary aliases.

Referring now to Figure 3F, an example of a user interface for configuring a security policy template for a specific NSD of a particular customer is shown. In particular, a filter rule for the available service ping is shown. In the illustrated embodiment, a WatchGuard service has also been defined to manage communications between the NSD and supervisor devices. Configuring the NSD can include specifying Contact Information for the customer (*e.g.*, company name, contact person, customer ID, etc.), Identification and Access information (*e.g.*, the NSD name and serial number, the NSD external IP address, a modem number that is used by the NSD, etc.), Network Configuration information (*e.g.*, IP addresses for the default gateway and for the trusted, external and optional interfaces, as well as hosts and networks related to each of the interfaces), Out Of Band (OOB) information to specify how to communicate with the NSD in ways other than through the external network (*e.g.*, via a modem or serial port), Route information (*e.g.*, network routing information when the customer uses a router to connect one or more secondary networks to a network behind the NSD), Authentication information to specify how user and/or device authentication will be performed, Log Host information about the one or more supervisor devices associated with the NSD (*e.g.*, a list of supervisor devices in order of precedence, with the primary supervisor device first, as well as password and other access information needed to interact with the devices), and Miscellaneous information such as the current time zone.

Figures 3G and 3H provide exemplary information related to events of interest and the specifying of network security information of interest. Referring first to Figure 3H, various configuration information for an HTTP proxy service is shown, including types of information which may be denied passage (*e.g.*, submissions, JAVA™ or ACTIVEX™ applets, and various types of information such as audio, images, text, and video) as well as whether to log network security information about accesses of the service.

Referring now to Figure 3G, a GUI is shown for specifying how to generate network security information, such as for a filter rule or service, and how to notify indicated users or devices of the network security information.

Those skilled in the art will appreciate that this information is provided for exemplary purposes only, and that the invention is not limited to the specific details discussed.

Figures 4A-4H provide an example of various network security information and NSD status information generated by implementing a specific security policy. Those skilled in the art will appreciate that network security information can include a variety of types of information about packets of interest, such as the direction, network interface, total length, protocol, header length, time to live, source IP address, destination IP address, source port, destination port, ICMP type and code, information about IP fragmentation, TCP flag bits, and IP options. The network security information can also include information about the logging itself, such as a time stamp, the action taken after applying filter rules, and information about the supervisor/host device such as the device name, corresponding process name, and corresponding process ID.

Those skilled in the art will also appreciate that this information is provided for exemplary purposes only, and that the invention is not limited to the specific details discussed.

Figures 5A-5D provide examples of a GUI displaying to a user of a manager device a hierarchical view of multiple supervisor devices and NSDs as well as corresponding configuration and network information.

Referring now to Figure 5A, a manager device ("Network Operations Center"), two supervisor devices ("WEP_1" and "WEP_2"), and seven NSDs ("Computer_Enterprises," "Bilington_Insurance," "General_Automotive," "Fields_Bank," "Starr_Manufacturing," "Vision_Cable," and "Gray_Design_Group") are illustrated in the upper left pane of the GUI. The first three NSDs are currently associated with the WEP_1 supervisor device, and the next four NSDs are currently associated with the WEP_2 supervisor device. The hierarchical arrangement allows devices to be accessed in a variety of ways, such as by selecting all of the security devices associated with a supervisor device by merely selecting or indicating the supervisor device. Note that supervisor devices and their associated security devices can be organized in a variety of ways, such as by geographical proximity or by conceptual similarity (*e.g.*, grouping customers based on similar types of business).

As is illustrated by the icons shown beside the devices in the left pane, a variety of information about the devices can be displayed graphically (*e.g.*, type of device and connection status). In addition, as is shown in the right pane of the GUI, various information about the supervisor devices and NSDs can be displayed textually (*e.g.*, the IP address, connection status, and phone number). The current contents of the right pane indicate that a variety of specific information can be displayed for a particular security device (in this example, "Computer_Enterprises"). Similarly, other information accessible to the device executing the GUI can be displayed, such as the available security policy templates shown in the lower left pane.

In addition to the currently displayed information, other tools and information can also be accessed via the GUI (*e.g.*, via the top-level menus, pop-up menus for particular displayed items, via the toolbar, etc.). For example, other available tools include the Security Management System (SMS) tool provides a GUI for viewing and modifying the existing security policy, as well as access to higher-level functions such as adjusting proxy settings, customizing web surfing rules and configuring a VPN. The SMS tool allows a user to specify access information for an NSD, examine or edit the configuration information of an NSD, save NSD configuration information either locally or on an NSD, add and delete services for the NSD, specify network-specific addresses for the NSD, set up logging and notification details about network security information, define default packet handling rules, block network information passing to or from certain IP addresses and port numbers, set up IP masquerading so that the NSD presents its IP address to the external network in lieu of any specific internal network addresses, set up port forwarding so that the NSD redirects incoming packets to a specific masqueraded device in the internal network based on the destination port numbers of the packets, determine the level of security for incoming and outgoing sessions using proxy services, and organize the internal network by defining aliases, defining groups of internal devices, and defining groups of users (*e.g.*, with different levels of access privileges).

Other tools also include the Status Viewer for retrieving specific status information about an NSD (*e.g.*, version information, uptime, memory usage, active connections, etc.), the Log Viewer for displaying network security information, the Host Watch for providing a graphical view of real-time connections between an NSD's trusted and external networks, the Service Watch for graphing the number of connections of service, the Mazameter for displaying real-time bandwidth usage for a particular NSD interface, and the Historical Reporting to run NSD reports related to exceptions (such as denied packets), usage by supervisor device, service, or session, time series reports, masquerading information reports, and URL reports.

Figure 5B provides an example of a GUI for a Host Watch tool that provides a graphical view of real-time connections, and Figures 5C and 5D provide examples of GUIs for a Status Viewer tool. Figure 5C indicates various users associated with specific IP addresses, and Figure 5D includes information about IP addresses and ports which are currently blocked.

Those skilled in the art will also appreciate that this information is provided for exemplary purposes only, and that the invention is not limited to the specific details discussed.

Figure 6 is an example of one or more NSD software components which can be distributed by a manager device to an NSD. In the illustrated embodiment, the NSD is a security appliance device capable of executing the Linux operating system. In addition to implementing a specific security policy that generates network security information, the NSD can also perform additional tasks, such as providing support for Virtual Private Networks (VPNs). The NSD software components include a version of the Linux OS kernel 610 which is capable of executing on the NSD to provide various OS functionality (*e.g.*, TCP/IP support, network drivers, etc.). The OS software component can also include an application programming interface (API) so that various other software components can interact with the OS kernel in a consistent manner.

One software component which interacts directly with the OS is the packet filter engine 615. The packet filter engine implements the specific security policy for the NSD, and interacts with various other software components including the firewall 630, proxies for various network services 635, and authentication software 640. The firewall component can provide a variety of functions such as configuring security policy filter rules, providing an interface to implement communication and access security (*e.g.*, via encryption), launching proxies for various network services, and communicating with management software of the NSD client (*e.g.*, a business which owns the trusted devices protected by the NSD). The firewall component can provide a client API 645 which client computers can contact, or can instead communicate with such an API provided by the client. The various network service proxies can provide a variety of information about the activities and configuration of the proxies, and the authentication software can ensure that users or devices provide the necessary access information before gaining access to the NSD or being able to receive information (*e.g.*, network security information) from the NSD.

Other software components which interact directly with the OS include various functionality-specific drivers (*e.g.*, VPN drivers) 620, and various service and protocol drivers (*e.g.*, TCP/IP driver) 625. Most functionality-specific drivers will also have a corresponding software component which implements the functionality and which interacts with the driver, such as the VPN software 650 interacting with driver 620. Similarly, one or more software components may be associated with the service and protocol drivers to implement or provide support for those protocols and services, such as the initialization program 655 interacting with drivers 625.

It is also possible for some software components to execute on the NSD in a manner such that they do not directly interact with other software components. For example, the network security information logging component 660 provides network security information to supervisor devices. While the logging component could interact with other components such as the packet filter engine to retrieve the network security information of interest, the logging component could also retrieve the information from a temporary local storage without such direct interaction. The logging component can provide a supervisor device API 670 which supervisor devices can contact, or can instead communicate with such an API provided by the supervisor devices. As with the firewall component and other components providing information or access to external devices, the logging component can provide for the security of the information it provides in a variety of ways (*e.g.*, encrypting the information before transmitting it).

Finally, as illustrated by the software components 670, a variety of other optional software components can be provided to and executed by an NSD. These components may or may not interact with other displayed software components. Those skilled in the art will appreciate that various of the displayed software components may interact with each other even if such interaction is not graphically illustrated, that existing software components could be removed, and that various software components could alternately be grouped together into a single component or separated into separate sub-components. In addition, those skilled in the art will appreciate that various specific types of software (*e.g.*, the Linux OS and the TCP/IP protocol) could be replaced with alternate types of software providing similar functionality.

Those skilled in the art will also appreciate that this information is provided for exemplary purposes only, and that the invention is not limited to the specific details discussed.

Figure 7 is an exemplary flow diagram of an embodiment of the Network Security Device routine 700. The routine implements a specific security policy for an NSD by monitoring network information passing between devices of interest (*e.g.*, between external devices and trusted devices), applying security policy filter rules when appropriate, and generating network security information about events of interest. In addition, the routine responds to management-related messages (*e.g.*, from supervisor devices) when appropriate.

The routine begins at step 705 where the NSD executes an initial boot program that loads the software to be executed by the NSD. After the software is loaded, the routine continues to step 710 to load various NSD-specific network packet filter rules that will be used to implement the specific security policy for the NSD, as well as any other NSD-specific configuration information. The software and NSD-specific configuration information will typically be stored in non-volatile memory (*e.g.*, flash RAM or a magnetic disk) by the NSD, but can also be loaded from a remote device.

After step 710, the routine continues to step 715 to monitor any passing network information. When network information packets of interest are detected, the routine continues to step 720 to filter the network information packets by executing the Filter Network Packets subroutine 720. After filtering the network information packets, the routine continues to step 725 to generate network security information about any events of interest by executing the Generate Network Security Information subroutine 725. The routine then continues to step 730 to respond to any management-related messages received (*e.g.*, from a supervisor device) by executing the Respond To Management Message subroutine 730. After step 730, the routine continues to step 790 to determine whether to continue monitoring network information packets. If so, the routine returns to step 715, and if not the routine ends at step 795.

Those skilled in the art will appreciate that network information can be monitored and altered in a variety of ways. In addition, network information can be specified in a variety of different types of packets, and can take a variety of forms other than packets. In addition, an NSD can be implemented in a variety of ways, such as by using a general-purpose computer executing specialized software or by using a special-purpose computer. For example, the Firebox10 and Firebox100 products from WatchGuard Technologies, Inc., of Seattle, WA, can be used to implement some aspects of an NSD.

Figure 8 is an exemplary flow diagram of an embodiment of the Filter Network Packets subroutine 720. The subroutine determines whether network information packets match one or more security policy 'filter rules, applies filter rules as appropriate to determine what actions to take for the packets, and then takes the appropriate action. The subroutine begins at step 805 where information about the network information packets of interest are received. The subroutine continues to step 810 to determine if the packets match one or more of the filter rules. If so, the subroutine continues to step 815 to apply one or more of the filter rules as appropriate to determine an action to be taken for the packets. For example, if multiple rules apply then only the rule with the highest precedence may be used, or alternately each matching rule may be applied in order of increasing or decreasing precedence.

If it is instead determined in step 810 that none of the filter rules apply, the subroutine continues to step 820 to determine a default action to be taken for the packets. A variety of types of default actions can be used, including denying passage of all packets that are not explicitly approved, blocking spoofing attacks, blocking port space probes, and blocking address space probes. After steps 815 or 820, the subroutine continues to step 825 to take the determined action on the packets. In the illustrated embodiments, the possible actions include denying or allowing the passage of the packet to the intended recipient. After step 825, the subroutine continues to step 895 and returns.

Those skilled in the art will appreciate that a network information security policy can be implemented in ways other than using filter rules. In addition, default filtering rules can be used such that some filter rules will apply to any packet. Moreover, a variety of actions can be taken on packets other than allowing or denying passage of the packets, including modifying the packets to add or remove information, or holding the packets until additional processing (*e.g.*, manual review) can be performed on the packets. In addition, additional actions may be necessary for the subroutine based on the format of the packets. For example, determining whether a packet matches a filter rule may require first stripping various network transmission information from the packet, and this information may need to be added back to the packet if the determined action for the packet is to allow its passage to its intended recipient.

Figure 9 is an exemplary flow diagram of an embodiment of the Generate Network Security Information subroutine 725. The subroutine determines whether an event of interest has occurred (*e.g.*, the application of a filter rule of interest or the detection of a packet matching predefined characteristics of interest such as corresponding to a particular network service), logs network security information about the event if appropriate, and notifies one or more specified entities about the event if appropriate. The subroutine encrypts information before it is transmitted so that it can be transmitted over an external network without fear of the information of interest being intercepted. The subroutine begins at step 905 where information about the network information packets of interest are received. The subroutine continues to step 910 to determine if the packets indicate an event of interest for which network security information is to be logged.

If it is determined in step 910 that the packets indicate an event of interest for which network security information is to be logged, the subroutine continues to step 915 to generate the network security information about the event, such as by extracting information of interest from the packet including the packet sender, intended packet recipient, packet direction, etc. The subroutine then continues to step 920 to determine the supervisor device currently associated with the NSD. The subroutine next determines in step 925 if the current supervisor device is available to receive network security information from the NSD. If not, the subroutine continues to step 930 to determine an alternate supervisor device to be the current supervisor device, and then returns to step 925 to determine if the new supervisor device is available. After a supervisor device is found to be available and designated as the current supervisor device, the subroutine continues to step 933 to encrypt the network security information in a manner accessible by the current supervisor device (*e.g.*, with an asymmetric public key for the supervisor device, or with a symmetric key available to all supervisor devices). The subroutine then continues to step 935 to send the encrypted network security information to the current supervisor device.

Any necessary access information (*e.g.*, passwords) can also be included with the sent information.

After step 935, or if it is instead determined in step 910 that the packets do not indicate an event of interest for which network security information is to be logged, the subroutine continues to step 940 to determine if the packets are of a type that require immediate notification of one or more entities (*e.g.*, users, devices, services, etc.). If so, the subroutine continues to step 945 to notify the designated entities in the appropriate manner, such as by using a predefined notification means (*e.g.*, email, a pager, voice mail, a message containing predefined information, etc.). This communication can also be encrypted as appropriate. After step 945, or if it is instead determined in step 940 that immediate notification of one or more entities is not required, the subroutine continues to step 995 and returns.

Those skilled in the art will appreciate that network security information can be sent to a supervisor device in alternate ways. For example, the NSD could store network security information until a sufficient amount was available before sending it to a supervisor, could send network security information on a periodic basis, could send network security information only when requested by a supervisor device, or could temporarily store network security information while the primary supervisor device or all supervisor devices are unavailable. In addition, network security information can be generated in a variety of ways and can include a variety of information, including sending the entire packets of interest, sending only some information from each packet, or sending only summary reports about multiple packets. In addition, events of interest which trigger the logging of network security information or the notification of some entity can be defined and identified in a variety of ways, such as any packets to or from a particular device or a device in a particular class of devices, any packets for which a specific action are taken (*e.g.*, deny passage), any packets containing contents of interest (*e.g.*, particular words or an attached file of a particular type), any packets corresponding to a particular type of network service (*e.g.*, HTTP requests), etc. Finally, a variety of means for providing security to information being transmitted over a non-secure network can be utilized, including symmetric keys, asymmetric keys, passwords, etc.).

Figure 10 is an exemplary flow diagram of an embodiment of the Respond To Management Messages subroutine 730. The subroutine determines whether the NSD has received a management-related message, determines whether the sender of the message is authorized to access management functions of the NSD, decrypts the message if necessary, and responds to the message when appropriate. The subroutine begins at step 1005 where information about the network information packets of interest are received. The subroutine continues to step 1010 to determine whether the packets contain a message that is directed to the NSD. If so, the subroutine continues to step 1015 to determine what access information (*e.g.*, passwords, the sender being on a list of authorized devices, etc.) is required for the message, as well as any information needed to decrypt the message if it is encrypted (*e.g.*, a password, or a public or private key). The subroutine continues to step sz17 to decrypt the message if it is encrypted. The subroutine then continues to step 1020 to verify whether the sender of the message has supplied any necessary access information and otherwise met any other access criteria.

If the necessary access has been verified, the subroutine continues to step 1025 to determine if the message is a request for information (*e.g.*, status of the NSD, NSD configuration information, or network security information), information being supplied (*e.g.*, a security policy template, NSD-specific configuration information, or NSD software), or some other instruction (*e.g.*, reboot the NSD so that new software is used). If it is determined in step 1025 that the message is a request for information, the subroutine continues to step 1030 to supply the requested information if possible, including encrypting the information before sending if appropriate (*e.g.*, if the intended recipient is able to decrypt the information, and the information is sensitive or if all communications are encrypted) and including any necessary access information. If it is determined in step 1025 that the message is information being supplied, the subroutine continues to step 1035 to store the information in the appropriate location. In addition, other actions may be taken automatically if appropriate, such as loading new software immediately if possible. If it is determined in step 1025 that the message is some other instruction, the subroutine continues to step 1040 to process the instruction if possible.

After steps 1030, 1035 or 1040, or if it was determined in step 1010 that the packets do not contain a message directed to the NSD or in step 1020 that the necessary access has not been verified, the subroutine continues to step 1095 and returns. Those skilled in the art will appreciate that a variety of types of messages can be supplied from a supervisor device, directly from a manager device, from another NSD, or from an internal device. In addition, management-related messages can include a variety of types of requests, information, and other instructions.

Figure 11 is an exemplary flow diagram of an embodiment of the Supervisor Device routine 1100. The routine implements a host device for one or more NSDs by receiving network security information of interest and storing the information until requested by a manager device, as well as assisting the manager device in distributing various information to the NSDs which are currently associated with the supervisor device.

The routine begins at step 1105 where the supervisor device executes an initial boot program that loads the software to be executed by the supervisor device. Those skilled in the art will appreciate that the software can be loaded from local or remote storage. After the software is loaded, the routine continues to step 1110 to wait for a message. After a message is received, the routine continues to step 1115 to decrypt the message if it is encrypted. The decryption can be done in a variety of ways, such as by retrieving decryption information based on the specific sender of the message or based on the type of sender (*e.g.*, NSD or manager device). The routine then continues to step 1120 to determine if the message is from an NSD. If so, the routine processes the message by executing the Process NSD Message subroutine 1125, and if not the routine processes the message by executing the Process Manager Or Supervisor Device Message subroutine 1130. After steps 1125 or 1130, the routine continues to step 1190 to determine whether to continue processing messages. If so, the routine returns to step 1110, and if not the routine ends at step 1195.

Those skilled in the art will appreciate that a supervisor/host device can be implemented in a variety of ways, such as by using a general-purpose computer executing specialized software or by using a special-purpose computer. For example, a general-purpose computer executing an operating system (*e.g.*, SOLARIS™ from Sun Microsystems) and executing software from WatchGuard Technologies, Inc., of Seattle, WA, such as the WatchGuard Event Processor software, can be used to implement such aspects of a supervisor/host device. In addition, those skilled in the art will appreciate that each supervisor/host device may be able to support a large number (*e.g.*, 500) of NSDs.

Figure 12 is an exemplary flow diagram of an embodiment of the Process NSD Message subroutine 1125. The subroutine stores network security information sent by NSDs, notifies the manager device if an NSD not previously associated with the supervisor device begins sending information, and processes other NSD requests as appropriate. The subroutine begins at step 1205 where it receives a decrypted copy of the message sent from the NSD. The subroutine continues to step 1210 to determine if the sending NSD is on the list of NSDs that are currently associated with the supervisor device. If not, the subroutine continues to step 1215 to add the NSD to the current list.

After step 1215, or if it was instead determined that the sending NSD is on the list of NSDs that are currently associated with the supervisor device, the subroutine continues to step 1220 where any NSDs that are shown on the current list but which are not currently associated with the supervisor device are removed from the current list. Whether a listed NSD is still associated with the supervisor device can be determined in a variety of ways, such as by removing NSDs from whom no messages have been received for a certain amount of time or by removing NSDs indicated to be associated with other supervisor devices (*e.g.*, by the NSD, the manager device, or the other supervisor device). The subroutine then continues to step 1225 where, if any NSDs have been added or removed, the manager device is notified of the changes in the current list of NSDs. As with other communications, this communication can be encrypted if appropriate and any necessary access information can be included in the message.

The subroutine then continues to step 1230 to determine if the message from the NSD is composed of network security information. If so, the subroutine continues to step 1235 to store the information in the log maintained by the supervisor device. The information in the log is encrypted before it is stored so that any other device able to access the log cannot obtain access to the contents of the stored network security information. If it is determined in step 1230 that the message from the NSD is not composed of network security information, the subroutine instead continues to step 1240 to process the message from the NSD as appropriate. For example, the NSD may be using the supervisor device as an intermediary when sending a message to another device such as the manager device, another NSD, or another supervisor device. After steps 1235 or 1240, the subroutine continues to step 1295 and returns.

Those skilled in the art will appreciate that NSD messages can be processed in a variety of alternate ways. For example, the list of NSDs may be purged on a periodic basis rather than when each new NSD message is received, and the manager device can be updated as to the changes in the list in a similar manner. In addition, each supervisor device can maintain a single log in which the network security information of multiple NSDs is stored, or can alternately maintain individual logs for each NSD. Similarly, if the supervisor device's log is not accessible to other devices, the information stored in the log file may not be encrypted, with the supervisor device instead encrypting the information before it is sent.

Figure 13 is an exemplary flow diagram of an embodiment of the Process Manager Or Supervisor Device Message subroutine 1130. The subroutine receives a copy of a message from the manager device that is to be distributed to multiple NSDs, and distributes a copy of the message to each of those NSDs which are currently associated with the supervisor device. The subroutine also receives requests from the manager device or another supervisor device, such as requests from the manager device for the various (potentially distributed) network security information of an NSD, and responds to the request if possible.

The subroutine begins at step 1305 where it receives a decrypted copy of the sent message. The subroutine then continues to step 1310 to determine if the intended recipients of the message include one or more NSDs. If so, the subroutine continues to step 1315 to send a copy of the message to each of the intended recipient NSDs which are on the list of NSDs currently associated with the supervisor device. As with other communications, the messages are sent in an encrypted manner if appropriate and any necessary access information is added to the message.

If it is instead determined in step 1310 that the received message is not intended for NSDs, the subroutine continues to step 1320 to determine if the message is a request from a manager device for the network security information of an NSD. If so, the subroutine continues to step 1325 to retrieve any portions of the requested information which are stored by the supervisor device in the log. The subroutine then continues to step 1330 to determine if any other supervisor devices store at least a portion of the requested information. This can be determined in a variety of ways, such as by receiving a list of all such supervisor devices from the manager device, by querying other supervisor devices if they store any of the requested information (*e.g.*, after analyzing the retrieved information and determining that it is not complete), by querying the NSD to determine to which supervisor devices the NSD has sent network security information, etc.

If it is determined in step 1330 that other supervisor devices store at least a portion of the requested information, the subroutine continues to step 1335 to contact those other supervisor devices and retrieve those portions of the information. The subroutine then continues to step 1340 to combine the various portions of network security information together. After step 1340, or if it was determined in step 1330 that other supervisor devices do not store at least a portion of the requested information, the subroutine sends the retrieved network security information to the requester in step 1345.

As with other communications, the network security information is encrypted and the necessary access information is supplied with the information.

The encryption of the network security information to be sent to the manager device can be handled in a variety of ways. If the other supervisor devices from which information is retrieved also encrypt the information stored in their logs, the information can be sent to the requesting supervisor device without decrypting the information. If the manager device is able to decrypt the various portions of the network security information encrypted by different supervisor devices (*e.g.*, if all supervisor devices use the same key for encryption), then the requesting supervisor device can just forward the various encrypted portions of information to the manager device. Alternately, if the requesting supervisor device can decrypt the information from the various other supervisor devices, the requesting supervisor device can combine all of the network security information in a decrypted form and then encrypt the information before sending it to the manager device. Yet another option is for each of the other supervisor devices to encrypt their network security information before sending it to the requesting supervisor device, with the encryption such that the requesting supervisor device can decrypt it (*e.g.*, by using the public key of the requesting supervisor device). Those skilled in the art will appreciate that other methods of sending this information are readily apparent.

If it was instead determined in step 1320 that the message received by the supervisor device is not a request from a manager device for the network security information of an NSD, the subroutine continues to step 1350 to process the message as appropriate. For example, the message may be from another supervisor device that is gathering the network security information of an NSD in preparation for forwarding the information to the manager device. In this situation, the supervisor device forwards the requested network security information to the other supervisor device. After steps 1315, 1345 or 1350, the subroutine continues to step 1395 and returns.

Those skilled in the art will appreciate that requests for network security information may be for amounts of information other than all available information, such as information generated during a specified time period or information of a certain type. In such situations, only the information requested can be returned, or instead all available information can be returned and the requester can extract the desired information. In addition, when sending information to multiple NSDs that are currently associated with multiple supervisor devices, the manager device could send a single message to a single supervisor device (rather than a single message to each of those supervisor devices) and have the single supervisor device distribute the message as necessary to the other supervisor device, or to other NSDs with which the supervisor device is not currently associated.

Figures 14A and 14B are exemplary flow diagrams of an embodiment of the Manager Device routine. The routine executes on the manager device, and receives messages from supervisor devices such as indications of the supervisor devices currently associated with NSDs that are being managed by the manager device. The manager device also receives a variety of user commands related to managing the NSDs and supervisor devices, and processes the commands as appropriate.

The routine begins at step 1405 where a graphical user interface (GUI) is displayed to the user. This display provides a hierarchical tree view of the various supervisor devices and the NSDs which are associated with each supervisor device. A variety of other types of information can also be conveyed, such as the status of supervisor devices (*e.g.*, available or unavailable), the status of NSDs, the flow of information that is occurring between devices, etc. The GUI also allows the user to easily enter management-related commands, and to display information of interest such as the aggregated network information of one or more NSDs. After step 1405, the routine continues to step 1410 to wait for a user command or for a message.

After receiving a user command or message, the routine continues to step 1415 to determine if a user command was received. If not, the routine continues to step 1420 to determine if the received message is an indication of a current association between an NSD and a supervisor device, such as after a fail-over when the indicated supervisor device became the current supervisor device for an NSD after the primary supervisor device for the NSD was unavailable. If it is determined in step 1420 that the received message is an indication of a current association between an NSD and a supervisor device, the routine continues to step 1425 to store the association information. If it is determined in step 1420 that the received message is not an indication of a current association between an NSD and a supervisor device, the routine continues to step 1430 to process the message as appropriate.

If it was instead determined in step 1415 that a user command was received, the routine continues to step 1435 to determine if the command is to create or modify a security policy template. If so, the routine continues to step 1440 to display a list of possible network services and protocols that may be of interest. The routine then continues to step 1445 where the user can indicate one or more services or protocols for which filter rules are to created. For each service or protocol, the user specifies the specific characteristics which network information packets must have to match the rule (*e.g.*, from a specific sender to any recipient, or incoming messages from any device of a specified type or class). The user also specifies the appropriate action to be taken with network information packets that satisfy the rule. The user can also specify aliases which are to be customized with NSD-specific configuration information when the template is loaded on a particular NSD. For example, if the user defines one or more filter rules related to an internal HTTP server, an alias can be created that will eventually hold the NSD-specific information about the particular HTTP server. After the filter rules and other information of the security policy template are defined or modified, the security policy template is stored.

If it was instead determined in step 1435 that the command is not to create or modify a security policy template, the routine continues to step 1450 to determine if the command is to distribute a security policy template to one or more NSDs. If so, the routine continues to step 1455 to receive an indication from the user of the template to be distributed, and to then retrieve a copy of the indicated template. If it was instead determined in step 1450 that the command is not to distribute a security policy template to one or more NSDs, the routine continues to step 1460 to determine if the command is to distribute one or more software components to one or more NSDs. If so, the routine continues to step 1462 to receive an indication from the user of the software components to be distributed, and to then retrieve copies of the indicated software components. After steps 1455 or 1462, the routine continues to step 1464 to receive from the user an indication of the NSDs to receive either the template or the software components. The routine continues to step 1466 to determine the one or more supervisor devices currently associated with the indicated NSDs, and then continues to step 1468 to send a single copy of the information to be distributed to each of the determined supervisor devices. The copy of the information sent to the supervisor devices includes an indication of the NSDs that are to receive the information being distributed.

If it was instead determined in step 1460 that the command is not to distribute one or more software components, the routine continues to step 1470 to determine if the command is to configure an NSD by supplying NSD-specific information to customize a security policy template. If so, the routine continues to step 1472 to receive an indication of the NSD to be configured. The routine then continues to step 1474 to receive an indication from the user of the NSD-specific information which is to be used to configure the NSD. The routine then determines in step 1476 the supervisor device that is currently associated with the NSD, and in step 1478 sends the NSD-specific information to the supervisor device for forwarding to the NSD. Those skilled in the art will appreciate that rather than merely sending the information to the NSD, the supervisor device could send instructions to the NSD to load or modify the configuration of the NSD in an appropriate manner.

If it was instead determined in step 1470 that the command is not to configure an NSD, the routine continues to step 1480 to determine if the command is to retrieve aggregated network security information from an NSD. If so, the routine continues to step 1482 to receive an indication of the NSD. The routine then continues to step 1484 to determine the supervisor device that is currently associated with the NSD, and in step 1485 determines all supervisor devices which store network security information for the NSD. The routine then continues to step 1486 to notify the current supervisor device to retrieve the network security information of interest for the NSD, including indicating to the current supervisor device the other supervisor devices which may store portions of the network security information. The routine then continues to step 1487 to wait for the network security information. After receiving the network security information, the routine in step 1488 aggregates the network security information as appropriate. Those skilled in the art will appreciate that the network security information can be aggregated in a variety of ways, either automatically or in response to user indications.

If it was instead determined in step 1480 that the command is not to retrieve aggregated network security information, the routine continues to step 1490 to process the command if appropriate. After steps 1425, 1430, 1445, 1468, 1478, 1488, or 1490, the routine then continues to step 1492 to determine whether to continue processing messages and commands. If so, the routine returns to step 1410, and if not the routine ends at step 1495.

Those skilled in the art will appreciate that a manager device can be implemented in a variety of ways, such as by using a general-purpose computer executing specialized software or by using a special-purpose computer. For example, a general-purpose computer executing an operating system (*e.g.*, WINDOWS 95™ or WINDOWS NT™ from Microsoft Corp.) and executing software from WatchGuard Technologies, Inc., of Seattle, WA, such as the Global Policy Manager, Graphical Monitor, Historical Reporting Module, Global Console, WebBlocker, Branch Office VPN, Network Configuration Wizard and Security Management System (SMS) Control Center software components, can be used to implement some aspects of a manager device.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

CLAIMS

1. A method for managing a security device by collecting security information generated by the security device, the generated security information based on network information passing between other network devices, the generated security information stored on at least one host device distinct from the security device, the method comprising:

receiving a request for the generated security information;

determining the host devices on which at least portions of the generated security information are stored; and

when there are multiple determined host devices,

for each of the multiple determined host devices, retrieving the portions of the generated security information that are stored on the host device; and

aggregating the retrieved portions of the generated security information.

2. The method of claim 1 including determining a host device that is a primary host device for the security device, and wherein the portions of the generated security information from each of the multiple determined host devices are retrieved from the primary host device after the primary host device collects the portions from the multiple determined host devices.

3. The method of claim 1 including requesting from each of the multiple determined host devices the portions of the generated security information that are stored on the host device.

4. The method of claim 1 wherein the aggregating of the retrieved portions of the generated security information includes sorting the aggregated security information chronologically.

5. The method of claim 1 wherein the aggregating of the retrieved portions of the generated security information includes sorting the aggregated security information by type of security information.

6. The method of claim 1 wherein the received request for the generated security information is from a user, and including displaying the aggregated security information to the user.

7. The method of claim 1 including determining a change needed in network information allowed to pass between the other network devices based on the aggregated security information.

8. The method of claim 1 including displaying to a user a view including the security device and the host devices, and wherein the request for the generated security information involves a visual indication by the user of the security device.

9. The method of claim 1 wherein a plurality of network security devices are managed by a security manager device with a plurality of supervisor devices, and wherein each of the network security devices generates collectable network security information that is related to an associated group of network devices, stores the generated network security information on a primary supervisor device for the network security

device when the primary supervisor device is available to store the generated network security information, and stores the generated network security information on an alternate supervisor device when the primary supervisor device is unavailable.

10. The method of claim 9 wherein the generating of the network security information includes, for each network security device:

monitoring network information passing between any network device in the associated group for the network security device and any network device not in the associated group; and

when the monitored network information is of an indicated type,

determining whether the primary supervisor device for the network security device is available to receive information;

when the primary supervisor device is available, sending network security information about the monitored network information to the primary supervisor device for storage; and

when the primary supervisor device is not available, sending network security information about the monitored network information to an alternate supervisor device for storage.

11. The method of claim 10 wherein for each network security device, a security policy for the network security device specifies the indicated types of monitored network information for which to generate network security information and specifies data related to the monitored network information to be included in the generated network security information.

12. The method of claim 9 including:

distributing security control information to multiple network security devices, the security control information to be used to generate network security information, by:

determining a supervisor device that is the primary supervisor device for each of the multiple network security devices;

sending a single copy of the security control information to the determined supervisor device; and

indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices; and

aggregating the network security information generated by an indicated one of the multiple network security devices using the security control information, by:

determining at least one alternate supervisor device that stores at least a portion of the network security information generated by the indicated network security device;

notifying the primary supervisor device for the indicated network security device of a desire for the generated network security information, the notifying including an indication of the determined alternate supervisor devices; and

in response, receiving the generated network security information.

13. The method of claim 12 wherein the distributed security control information is software to be executed by the multiple network security devices to control the generation of the network security information.

14. The method of claim 12 wherein the distributed security control information is a security policy template that defines the network security information to be generated, and including:

after a copy of the security policy template has been sent to each of the multiple network security devices, configuring each copy of the security policy template with information specific to the network security device to which the security policy template was sent.

15. The method of claim 12 wherein after the notifying of the primary supervisor device, the primary supervisor device sends the generated network security information to the manager device by:

retrieving from each of the determined alternate supervisor devices the network security information generated by the indicated network security device;

retrieving any network security information generated by the indicated network security device that is stored by the primary supervisor device; and

sending the retrieved network security information to the manager device.

16. The method of claim 12 including, after the receiving of the generated network security information, aggregating the portions of the generated network security information stored by the determined alternate supervisor devices and any portion of the generated network security information stored by the primary supervisor device.

17. The method of claim 12 including displaying to a user the plurality of network security devices and the plurality of supervisor devices in such a manner that the primary supervisor device for each of the network security devices is visually indicated, and wherein the distributing of the security control information to the multiple

network security devices is in response to selection by the user of the displayed multiple network security devices.

18. The method of claim 9 wherein information is sent between the manager device and the supervisor devices and between the supervisor devices and the network security devices in a secure form so that others do not have access to contents of the information.

19. The method of claim 1 wherein the generated security information is stored on multiple host devices distinct from the security device, wherein the received request is from a manager device, wherein the determining of the host devices includes receiving an indication of the multiple host devices, and including sending to the manager device the retrieved portions of the generated security information.

20. The method of claim 19 including:

before sending to the manager device the retrieved portions of the generated security information, determining that the manager device is predefined as being authorized to receive the generated security information.

21. The method of claim 19 including:

receiving from the manager device access information; and

before sending to the manager device the retrieved portions of the generated security information, determining that the access information authorizes a sender of the access information to receive the generated security information.

22. The method of claim 19 including:

before sending to the manager device the retrieved portions of the generated security information, formatting the retrieved portions in a manner accessible only to the manager device.

23. The method of claim 19 wherein the indication of the multiple host devices is received from the manager device.

24. The method of claim 19 including, before receiving the indication of the multiple host devices, contacting the security device to determine the multiple host devices.

25. The method of claim 1 including, before the collecting of the generated security information, storing the generated security information in a distributed manner so as to ensure that the generated security information is available, the method comprising:

identifying whether a primary supervisor device for the security device is available to store received security information;

when the primary supervisor device is available, storing the security information on the primary supervisor device; and

when the primary supervisor device is not available, storing the security information on an alternate supervisor device.

26. The method of claim 25 including generating the security information by:

retrieving a policy which indicates types of network information;

monitoring the network information passing between the network devices; and

when the monitored network information is of a type indicated by the policy, generating security information about the monitored network information.

27. The method of claim 26 wherein the policy for the network security device indicates types of information to be included in the generated security information.

28. The method of claim 25 including:

before storing the security information on a supervisor device, determining that the supervisor device is predefined as being authorized to receive the security information.

29. The method of claim 25 including:

before storing the security information on a supervisor device, formatting the security information in a manner accessible only to the supervisor device.

30. The method of claim 25 wherein the storing of the generated security information is performed by the security device, and including sending the security information to the supervisor device that will store the security information in a manner accessible only to the supervisor device.

31. The method of claim 1 including distributing security policy implementation information to multiple security devices for use in implementing a security policy, comprising:

for each of the security devices, determining a supervisor device currently associated with the security device;

distributing the security policy implementation information to each of the determined supervisor devices; and

indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated.

32. The method of claim 31 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

33. The method of claim 31 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

34. The method of claim 33 including:

after the security policy implementation information has been distributed to each of the security devices, configuring the security policy implementation information distinctly on each security device.

35. The method of claim 31 wherein the security policy implementation information is an instruction to be executed by the multiple security devices related to the implementing of the security policy.

36. The method of claim 31 wherein the security policy implementation information is information common to the multiple security devices, and wherein for each of the multiple security devices the common information is for configuring a security policy template for the security device with information specific to the security device.

37. The method of claim 31 wherein before the security policy implementation information is distributed to each of the multiple security devices, at least some of the multiple security devices have existing security policy implementation information of a similar type, and wherein for those security devices the security policy implementation information to be distributed will replace the existing security policy implementation information.

38. The method of claim 31 wherein before the security policy implementation information is distributed to each of the multiple security devices, at least some of the multiple security devices have existing security policy implementation information of a similar type, and wherein for those security devices the security policy implementation information to be distributed will supplement the existing security policy implementation information.

39. The method of claim 31 wherein the distributing of the security policy implementation information to each of the determined supervisor devices is performed in a manner such that the security policy implementation information is not accessible to other devices.

40. The method of claim 31 including displaying to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and wherein the distributing of the security policy implementation information is in response to a visual selection by the user.

41. The method of claim 1 wherein a supervisor device distributes security policy implementation information to multiple security devices for use in implementing a security policy, by:

receiving from a manager device a single copy of security policy implementation information to be distributed to multiple security devices; and

for each of the multiple security devices, if the supervisor device is associated with the security device, distributing the security policy implementation information to the security device.

42. The method of claim 41 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

43. The method of claim 41 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

44. The method of claim 43 including:

after the security policy implementation information has been distributed to each of the security devices, configuring the security policy implementation information distinctly on each security device.

45. The method of claim 43 including:

before the security policy implementation information has been distributed to each of the security devices, for each security device configuring distinctly for that device a copy of the security policy implementation information that is to be distributed to that device.

46. The method of claim 43 including:

for each of the security devices, sending to the security device a control instruction indicating an action to be taken with the security policy implementation information by the security device.

47. The method of claim 41 wherein the security policy implementation information is an instruction to be performed by the security devices related to the implementing of the security policy.

48. The method of claim 41 wherein the supervisor device distributes the security policy implementation information to a security device only when the supervisor device is associated with the security device as a primary supervisor device for the security device.

49. The method of claim 41 including when the supervisor device is not associated with one of the multiple security devices, distributing the security policy implementation information to another supervisor device to be distributed to the one security device.

50. The method of claim 1 including distributing control information to multiple security devices for use in controlling operation of the multiple security devices, comprising:

for each of the security devices, determining a supervisor device currently associated with the security device;

distributing the control information to each of the determined supervisor devices; and

indicating to each of the determined supervisor devices to distribute the control information to the security devices with which the supervisor device is associated.

51. The method of claim 50 wherein after the control information is distributed to the security devices, the security devices operate in accordance with the control information.

52. The method of claim 1 wherein a security device operates in accordance with security policy implementation information distributed from a manager device by:

receiving security policy implementation information to be used in implementing a security policy; and

using the security policy implementation information to implement the security policy.

53. The method of claim 52 wherein the security policy implementation information is distributed to multiple security devices via a supervisor device associated with the multiple security devices.

54. The method of claim 52 wherein the security policy implementation information is software to be executed by the security device to control the implementing of the security policy.

55. The method of claim 52 wherein the security policy implementation information is a security policy template that indicates security information to be generated.

56. The method of claim 55 including:

after the security policy implementation information has been received, receiving from the manager device configuration information specific to the security device to customize the security policy template.

57. The method of claim 52 wherein the security policy implementation information is an instruction to be taken by the security device related to the implementing of the security policy.

58. The method of claim 52 including:

before using the security policy implementation information to implement the security policy, determining that the manager device is predefined as being authorized to distribute the security policy implementation information.

59. The method of claim 52 including:

receiving from the manager device access information; and

before using the security policy implementation information to implement the security policy, determining that the access information authorizes a sender of the access information to distribute the security policy implementation information.

60. The method of claim 1 including displaying to a user a view including the security device and the host devices, and wherein the received request is

based on a visual indication from the user of a security device from which to retrieve generated security information.

61. The method of claim 60 including displaying to the user the aggregated generated security information.

62. The method of claim 60 wherein the view of the security device and of the host devices includes a visual indication of a host device that is a primary host device for the security device.

63. The method of claim 60 wherein the view of the security device and of the host devices includes visual indications of the determined host devices.

64. The method of claim 60 wherein a visual indication displayed in the view of a device performing the method is modified to indicate that the generated security information has been retrieved.

65. The method of claim 1 including distributing security policy implementation information to multiple security devices for use in implementing a security policy by:

displaying to a user a view of the multiple security devices and of multiple supervisor devices;

receiving from the user visual indications of multiple security devices to which the security policy implementation information is to be distributed;

distributing the security policy implementation information to a supervisor device associated with each of the security devices; and indicating to the associated supervisor device to distribute the security policy implementation information to each of the security devices.

66. The method of claim 65 including:

displaying to the user multiple pieces of security policy implementation information; and

determining the security policy implementation information to be distributed based on a visual indication by the user.

67. The method of claim 65 wherein the view of the security devices and of the supervisor devices includes a visual indication of a supervisor device that is a primary host device for the security device.

68. The method of claim 65 wherein a visual indication for each of the multiple security devices is modified to indicate receipt by the security device of the security policy implementation information.

69. The method of claim 1 including displaying the generated security information to a user by:

displaying to the user a view including the security device and the host devices;

receiving from the user an indication of a security device from which to retrieve generated security information; and

displaying to the user an aggregation of the portions of the generated security information retrieved from the multiple host devices.

70. The method of claim 69 wherein the view of the security device and of the host devices includes visual indications of the multiple host devices.

71. The method of claim 69 wherein a visual indication displayed in the view of a device performing the method is modified to indicate that the generated security information has been retrieved.

72. The method of claim 1 including distributing security policy implementation information to multiple security devices for use in implementing a security policy by:

displaying to a user a view of a manager device, the multiple security devices and of multiple supervisor devices;

receiving from the user indications of multiple security devices to which the security policy implementation information is to be distributed; and

displaying to the user an indication that the security policy implementation information is distributed to the multiple security devices, the distribution accomplished by the manager device sending the security policy implementation information to a supervisor device associated with each of the security devices and indicating to the associated supervisor device to distribute the security policy implementation information to each of the security devices.

73. The method of claim 72 including:

displaying to the user multiple pieces of security policy implementation information; and

determining the security policy implementation information to be distributed based on a visual indication by the user.

74. The method of claim 72 wherein the view of the security devices and of the supervisor devices includes a visual indication that the associated supervisor device distributes the security policy implementation information to each of the security devices.

75. The method of claim 72 wherein a visual indication for each of the multiple security devices is modified to indicate receipt by the security device of the security policy implementation information.

76. The method of claim 72 wherein the multiple security devices to which the security policy implementation information is to be distributed are indicated from a selection by the user of the associated supervisor device.

77. A computer-readable medium whose contents cause a manager device to manage security devices by distributing security policy implementation information to multiple security devices for use in implementing a security policy, by:

for each of the security devices, determining a supervisor device currently associated with the security device;

distributing the security policy implementation information to each of the determined supervisor devices; and

indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated.

78. The computer-readable medium of claim 77 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

79. The computer-readable medium of claim 77 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

80. The computer-readable medium of claim 79 wherein the contents further cause the manager device to, after the security policy implementation information has been distributed to each of the security devices, configure the security policy implementation information distinctly on each security device.

81. The computer-readable medium of claim 77 wherein the security policy implementation information is an instruction to be executed by the multiple security devices related to the implementing of the security policy.

82. The computer-readable medium of claim 77 wherein the contents further cause the manager device to display to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and wherein the distributing of the security policy implementation information is in response to a visual selection by the user.

83. The computer-readable medium of claim 77 wherein the contents further cause the manager device to collect security information generated by a security device, the generated security information based on network information passing between

other network devices, the generated security information stored on at least one host device distinct from the security device, by:

receiving a request for the generated security information;

determining the host devices on which at least portions of the generated security information are stored; and

when there are multiple determined host devices,

for each of the multiple determined host devices, retrieving the portions of the generated security information that are stored on the host device; and

aggregating the retrieved portions of the generated security information.

84. The computer-readable medium of claim 83 wherein the contents further cause the manager device to determine a host device that is a primary host device for the security device, and wherein the portions of the generated security information for each of the multiple determined host devices are retrieved from the primary host device.

85. The computer-readable medium of claim 83 wherein the aggregating of the retrieved portions of the generated security information includes sorting the aggregated security information chronologically.

86. The computer-readable medium of claim 83 wherein the received request for the generated security information is from a user, and wherein the contents further cause the manager device to display the aggregated security information to the user.

87. The computer-readable medium of claim 83 wherein the contents further cause the manager device to display to a user a view including the security device

and the host devices, and wherein the request for the generated security information involves a visual indication by the user of the security device.

88. A computer system for managing a security device by collecting security information generated by the security device, the generated security information based on network information passing between other network devices, the generated security information stored on at least one host device distinct from the security device, comprising:

a user interface component that receives from a user a request for the generated security information; and

a security information retriever that determines the host devices on which at least portions of the generated security information are stored, and that when there are multiple determined host devices, for each of the multiple determined host devices, retrieves the portions of the generated security information that are stored on the host device and aggregates the retrieved portions of the generated security information.

89. The computer system of claim 88 wherein the user interface component is capable of generating a graphical display of the aggregated security information.

90. The computer system of claim 88 wherein the user interface component is capable of generating a graphical display including a hierarchical view of the security device and the host devices, and wherein the user interface component is further for receiving a visual indication of the security device indicating the request for the generated security information of the indicated security device.

91. The computer system of claim 88 for further distributing security policy implementation information to multiple security devices for use in implementing a security policy, the computer system further comprising:

a security device associator for determining for each of the security devices a supervisor device currently associated with the security device; and

an information distributor for distributing the security policy implementation information to each of the determined supervisor devices, and for indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated.

92. The computer system of claim 91 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

93. The computer system of claim 91 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

94. The computer system of claim 91 wherein the user interface component is further for displaying to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and for receiving a visual selection by the user that controls the distributing of the security policy implementation information.

95. The computer system of claim 88 for further storing the generated security information in a distributed manner so as to ensure the security information is available, the computer system further comprising:

a storage identifier for identifying whether a primary supervisor device for the security device is available to store received security information; and

an information storer for storing the security information on the primary supervisor device if the primary supervisor device is available, and for storing the security information on an alternate supervisor device when the primary supervisor device is not available.

96. The computer system of claim 95 further comprising:

a security information generator for retrieving a policy which indicates types of network information, for monitoring the network information passing between the network devices, and for generating security information about the monitored network information when the monitored network information is of a type indicated by the policy.

97. The computer system of claim 95 further comprising:

a security component for determining that a supervisor device is predefined as being authorized to receive the security information before storing the security information on the supervisor device.

98. The computer system of claim 88 for further implementing a security policy in accordance with security policy implementation information distributed from a manager device, the computer system further comprising:

a security policy information receiver for receiving security policy implementation information to be used in implementing a security policy; and a security policy implementer for using the security policy implementation information to implement the security policy.

99. The computer system of claim 98 wherein the security policy implementation information is software to be executed by the security device to control the implementing of the security policy.

100. The computer system of claim 98 wherein the security policy implementation information is a security policy template that indicates security information to be generated.

101. The computer system of claim 98 further comprising:

a security component for determining that the manager device is predefined as being authorized to distribute the security policy implementation information before using the security policy implementation information to implement the security policy.

102. A generated data signal transmitted via a data transmission medium from a manager device to a supervisor device, the data signal including a single copy of security policy implementation information to be distributed by the supervisor device to multiple security devices, the security policy implementation information for use by the supervisor devices in implementing a security policy,

so that the manager device can efficiently distribute information to multiple security devices via a supervisor device.

103. The data signal of claim 102 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

104. The data signal of claim 102 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

105. The data signal of claim 102 including configuration information to be distributed by the supervisor device to at least one security device, the configuration information specific to the at least one security device, the configuration information for configuring distinctly for the at least one security device a copy of the security policy implementation information that is to be distributed to that device.

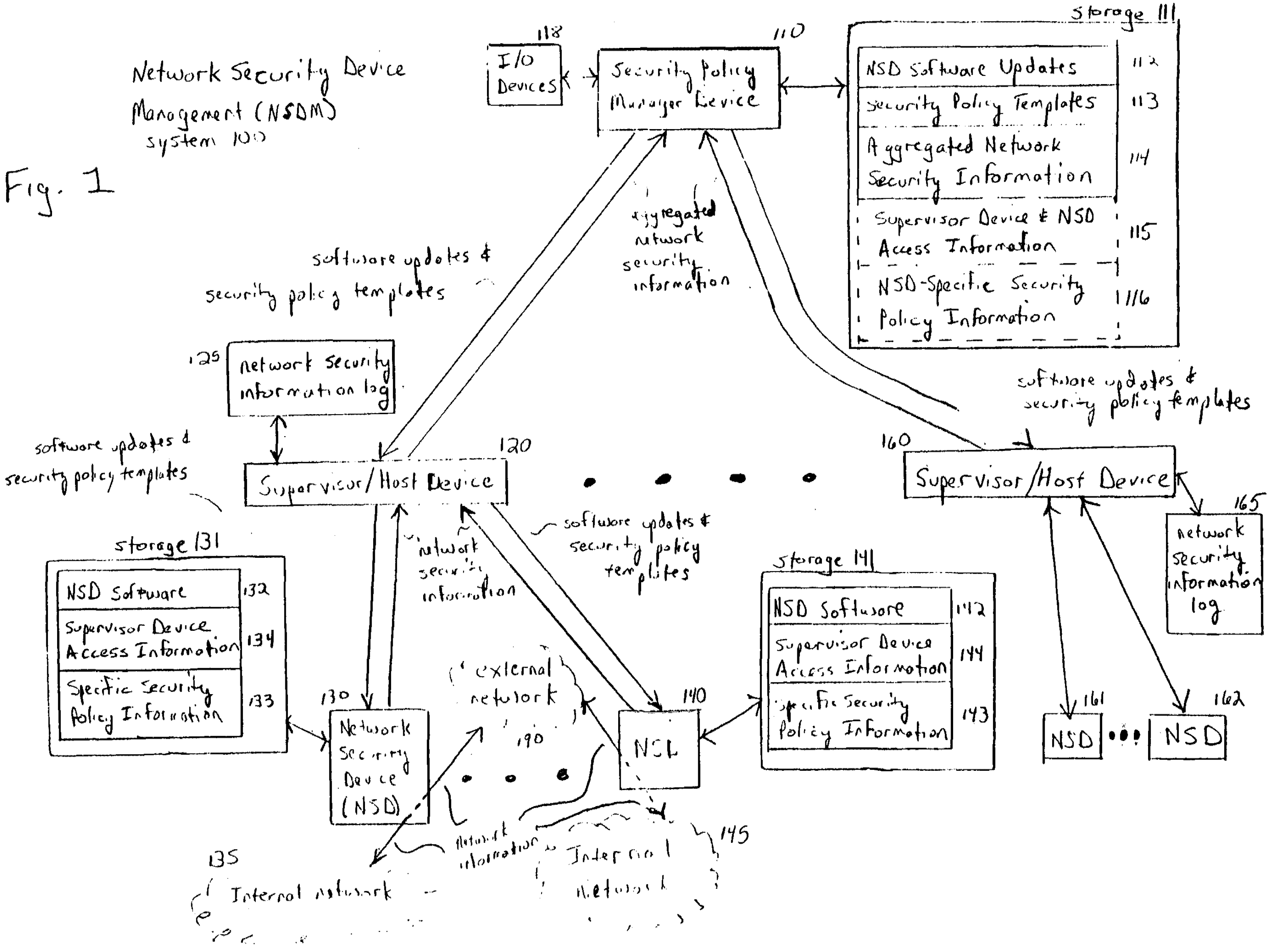
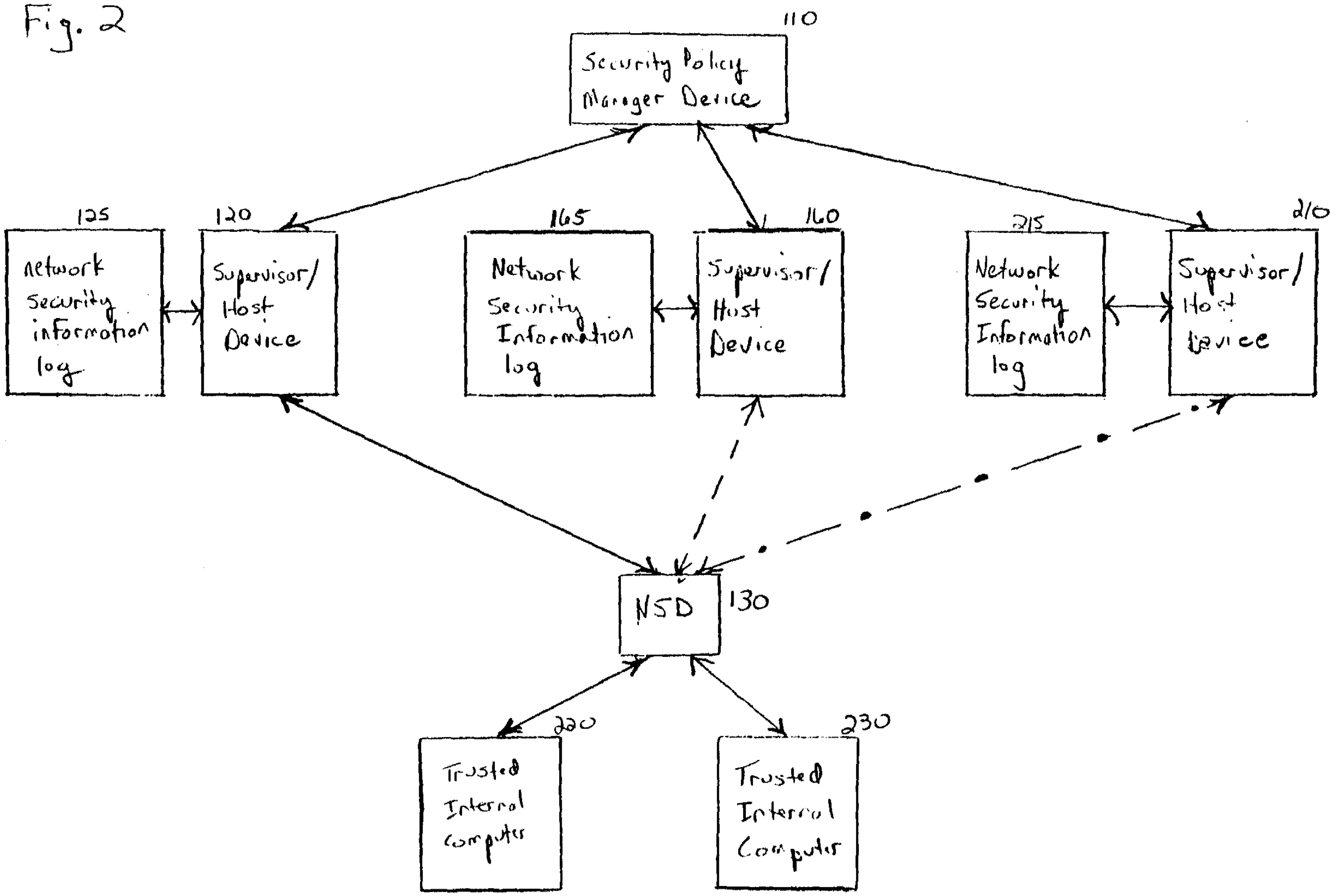

Network Security Device
Management (NSDM)
system 100
118
I/O Devices
110
Security Policy Manager Device
Storage 111
NSD Software Updates
112
Security Policy Templates
113
Aggregated Network Security Information
114
Supervisor Device & NSD Access Information
115
NSD-Specific Security Policy Information
116
software updates & security policy templates
aggregated network security information
software updates & security policy templates
125
network security information log
software updates & security policy templates
120
Supervisor/Host Device
160
Supervisor/Host Device
165
network security information log
network security information
software updates & security policy templates
storage 131
NSD Software
132
Supervisor Device Access Information
134
Specific Security Policy Information
133
130
Network Security Device (NSD)
external network
190
140
NSL
storage 141
NSD Software
142
Supervisor Device Access Information
144
Specific Security Policy Information
143
161
NSD
162
NSD
135
Internal network
Network information
145
Internal network

Fig. 1

Fig. 2


110
Security Policy Manager Device
125
Network Security information log
120
Supervisor/ Host Device
165
Network Security Information log
160
Supervisor/ Host Device
215
Network Security Information log
210
Supervisor/ Host Device
NSD
130
220
Trusted Internal computer
230
Trusted Internal Computer

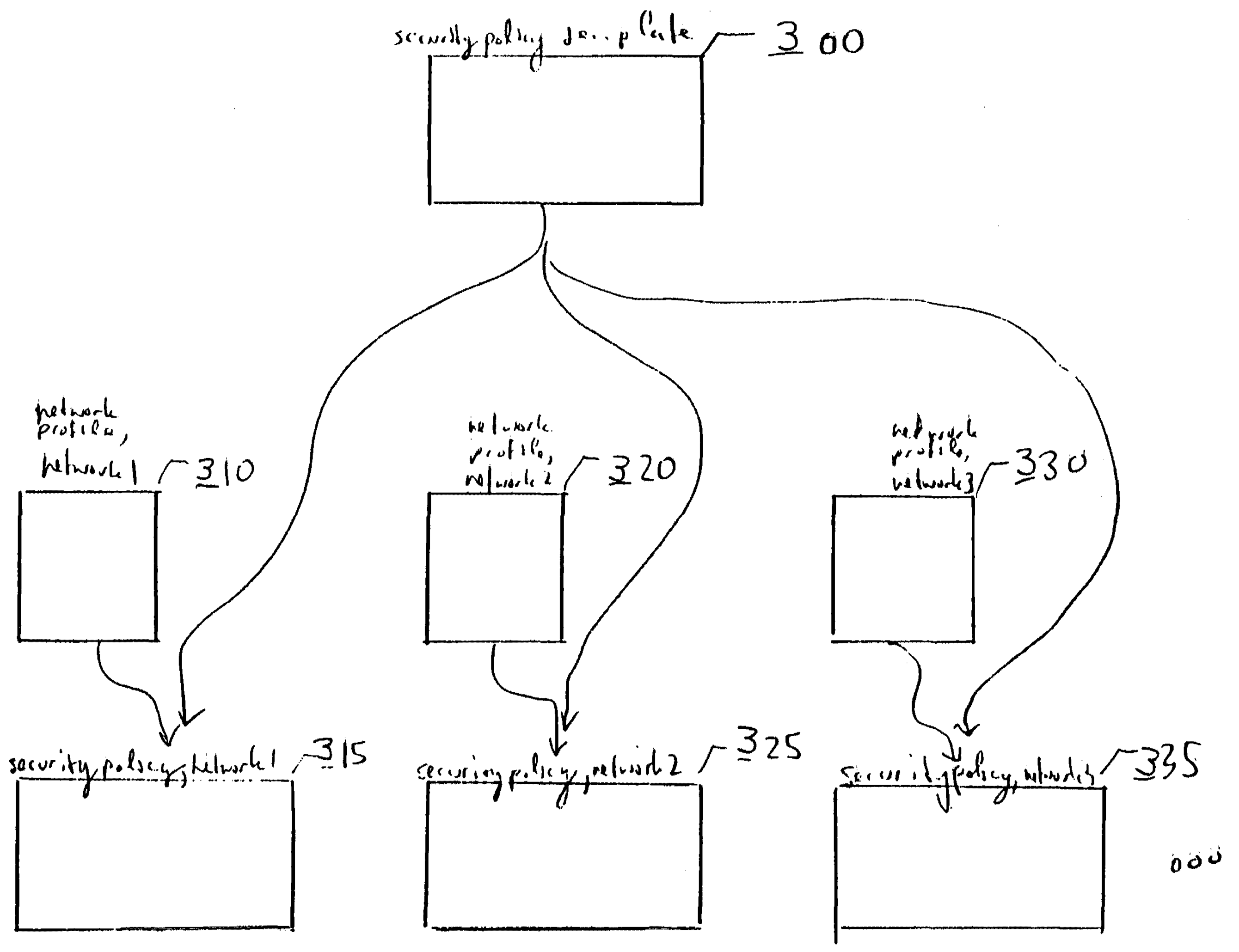

security policy template
300
network profile, network 1
310
network profile, network 2
320
network profile, network 3
330
security policy, network 1
315
security policy, network 2
325
security policy, network 3
335
ooo

FIG 3A

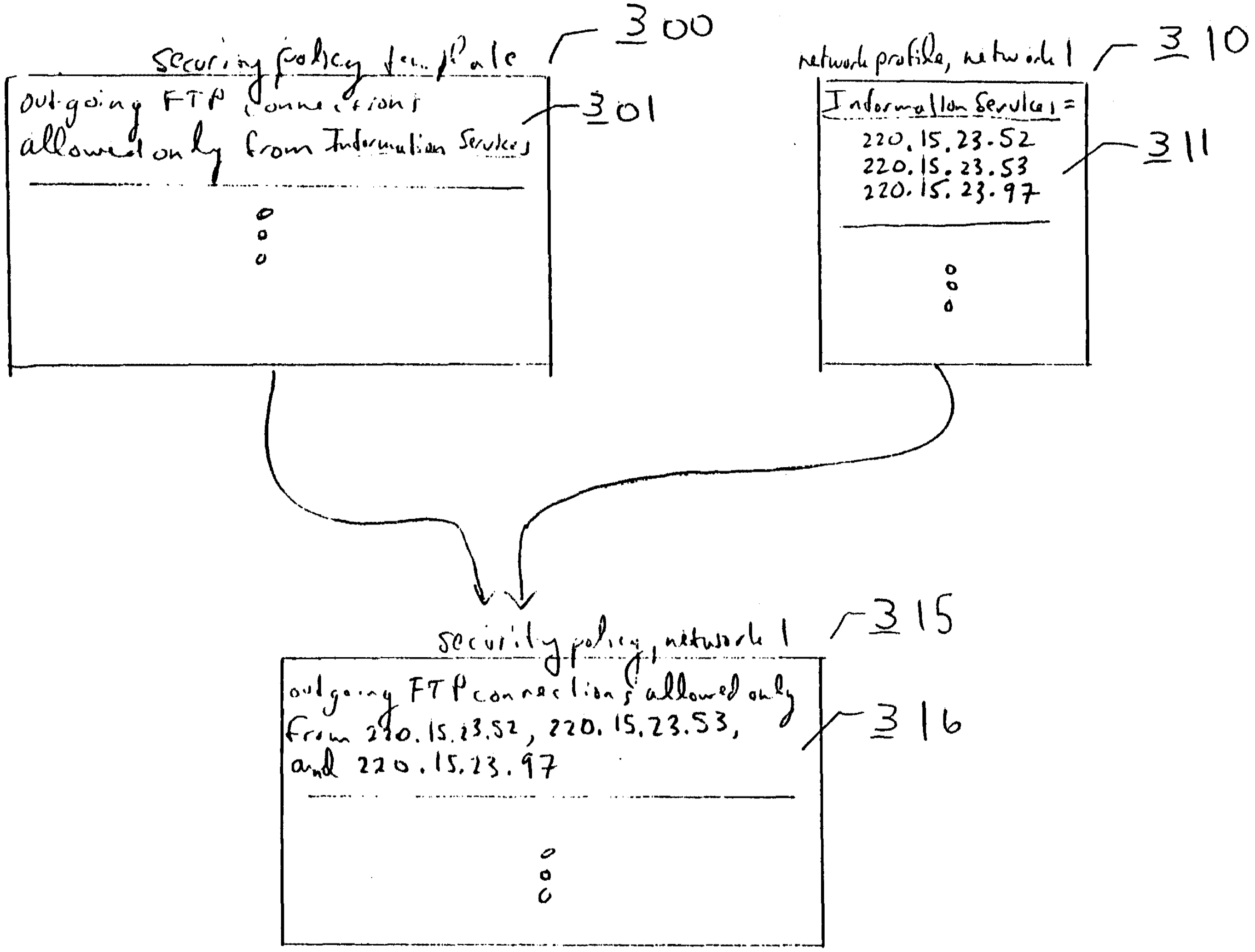
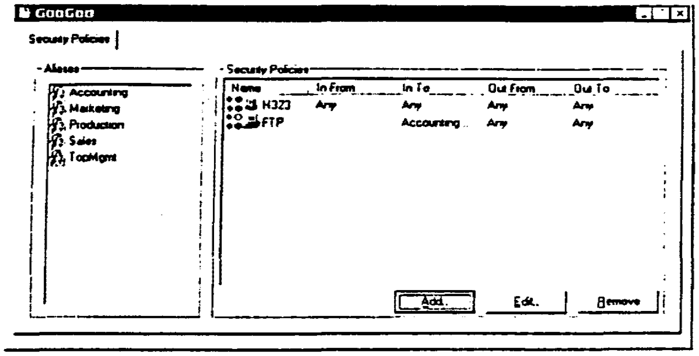
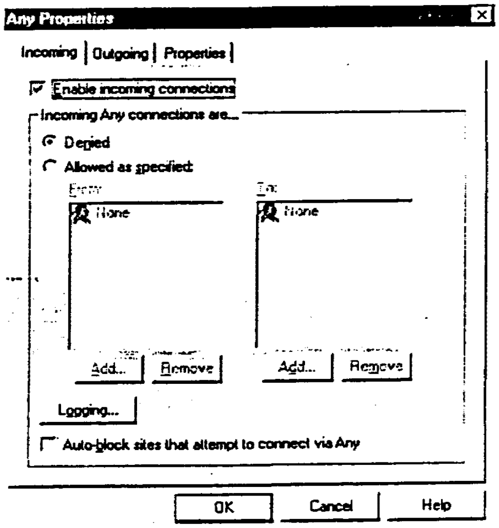

securing policy template
300
outgoing FTP connections allowed only from Information Services
301
network profile, network 1
310
Information Services =
220.15.23.52
220.15.23.53
220.15.23.97
311
security policy, network 1
315
outgoing FTP connections allowed only from 220.15.23.52, 220.15.23.53, and 220.15.23.97
316

Fig. 3 B



Name	In From	In To	Out From	Out To
H323	Any	Any	Any	Any
FTP		Accounting...	Any	Any

Fig. 3C



☑ Enable incoming connections

● Denied

○ Allowed as specified

□ Auto-block sites that attempt to connect via Any

Fig. 3D

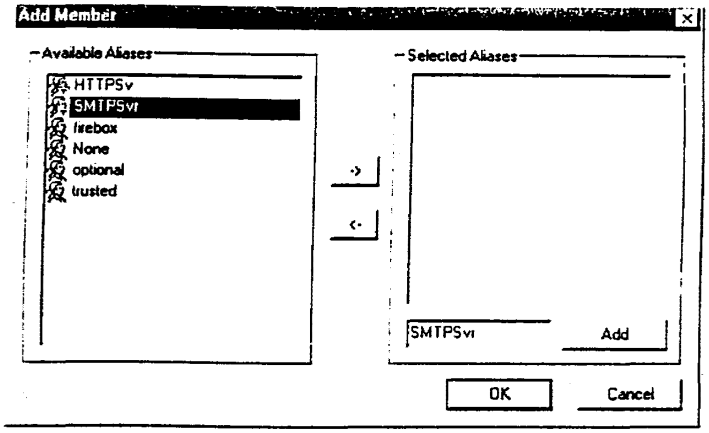
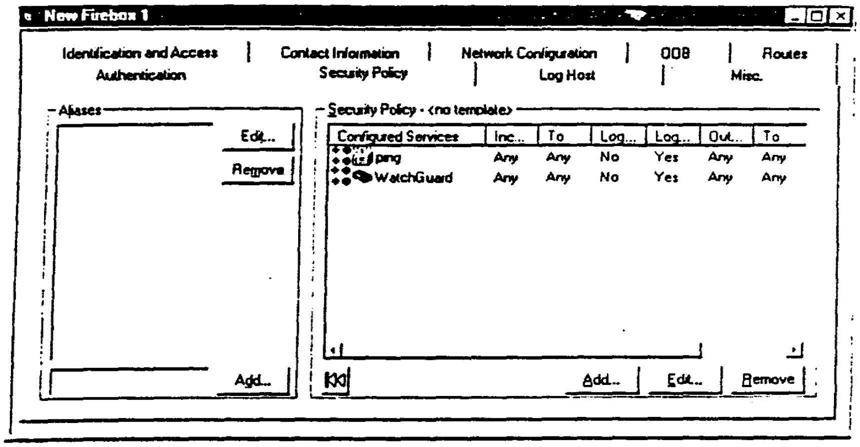


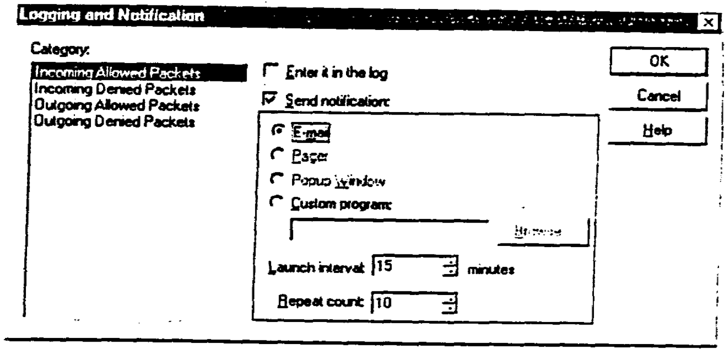
Fig. 3E



Security Policy - <no template>

Configured Services	Inc...	To	Log...	Log...	Out...	To
ping	Any	Any	No	Yes	Any	Any
WatchGuard	Any	Any	No	Yes	Any	Any

Fig. 3F

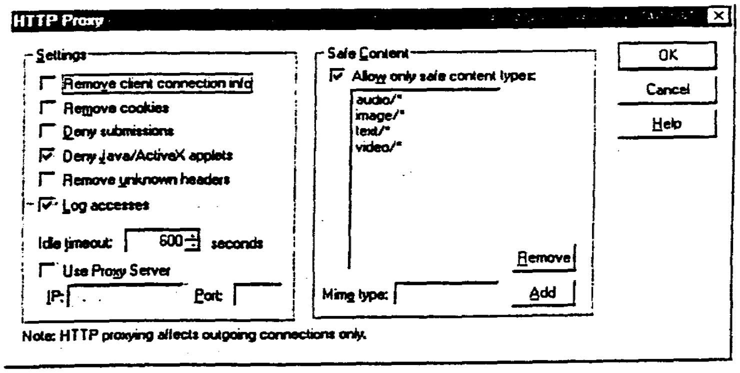


Category:
Incoming Allowed Packets
Incoming Denied Packets
Outgoing Allowed Packets
Outgoing Denied Packets

□ Enter it in the log
☑ Send notification:
● E-mail
○ Pager
○ Popup Window
○ Custom program:

Launch interval: 15 minutes
Repeat count: 10

Fig. 3G



Settings
□ Remove client connection info
□ Remove cookies
□ Deny submissions
☑ Deny Java/ActiveX applets
□ Remove unknown headers
☑ Log accesses
Idle timeout: 600 seconds
□ Use Proxy Server
IP: Port:

Safe Content
☑ Allow only safe content types:
audio/*
image/*
text/*
video/*
Mime type:

Note: HTTP proxying affects outgoing connections only.

Fig. 3H

Fig. 4A

```
Jun 15 14:28:15  controld: Firebox closed connection. Hard Close.
Jun 15 14:28:18  controld: WatchGuard controld 3.00.B120 (C) 1996-1998 Watchguard Technologies
Jun 15 14:28:10 10.1.1.1 vpnd [47]: WatchGuard vpnd v3.00.B120 (C) 1996-1998 WGTI
Jun 15 14:28:10 10.1.1.1 vpnd [47]: No VPN devices configured...exiting.
Jun 15 14:28:10 10.1.1.1 firewalld [48]: Explicitly set external interface was "", auto-detected "eth0"
Jun 15 14:28:10 10.1.1.1 init [1]: WatchGuard Init Copyright (C) 1996-1998 WatchGuard Technologies
Jun 15 14:28:10 10.1.1.1 kernel: Low memory threshhold at 95/90/88 percent.
Jun 15 14:28:10 10.1.1.1 kernel: Console: 16 point font, 400 scans
Jun 15 14:28:10 10.1.1.1 kernel: Console: colour VGA+ 80x25, 1 virtual console (max 63)
Jun 15 14:28:10 10.1.1.1 kernel: pcibios_init : BIOS32 Service Directory structure at 0x000fadc0
Jun 15 14:28:10 10.1.1.1 kernel: pcibios_init : BIOS32 Service Directory entry at 0xfb230
Jun 15 14:28:10 10.1.1.1 kernel: pcibios_init : PCI BIOS revision 2.10 entry at 0xfb260
Jun 15 14:28:10 10.1.1.1 kernel: Probing PCI hardware.
Jun 15 14:28:10 10.1.1.1 kernel: Warning : Unknown PCI device (1023:9660).  Please read include/linux/pci.h
Jun 15 14:28:10 10.1.1.1 kernel: Calibrating delay loop.. ok - 35.94 BogoMIPS
Jun 15 14:28:10 10.1.1.1 kernel: Memory: 15000k/16384k available (540k kernel code, 384k reserved, 460k data)
Jun 15 14:28:10 10.1.1.1 kernel: Swansea University Computer Society NET3.035 for Linux 2.0
Jun 15 14:28:10 10.1.1.1 kernel: NET3: Unix domain sockets 0.13 for Linux NET3.035.
Jun 15 14:28:10 10.1.1.1 kernel: Swansea University Computer Society TCP/IP for NET3.034
Jun 15 14:28:10 10.1.1.1 kernel: IP Protocols: ICMP, GRE, UDP, TCP
Jun 15 14:28:10 10.1.1.1 kernel: Checking 386/387 coupling... Ok, fpu using exception 16 error reporting.
Jun 15 14:28:10 10.1.1.1 kernel: Checking 'hlt' instruction... Ok.
Jun 15 14:28:10 10.1.1.1 kernel: Intel Pentium with F0 0F bug - workaround enabled.
Jun 15 14:28:10 10.1.1.1 kernel: alias mapping IDT readonly ... ... done
Jun 15 14:28:10 10.1.1.1 kernel: Linux version 2.0.33 (bryan@terror) (gcc version 2.7.2.1) #1 Wed Apr 22 12:00:23 PDT 1998
Jun 15 14:28:10 10.1.1.1 kernel: Starting kswapd v 1.2
Jun 15 14:28:10 10.1.1.1 kernel: Serial driver version 4.13 with no serial options enabled
Jun 15 14:28:10 10.1.1.1 kernel: tty00 at 0x03f8 (irq = 4) is a 16550A
Jun 15 14:28:10 10.1.1.1 kernel: tty01 at 0x02f8 (irq = 3) is a 16550A
Jun 15 14:28:10 10.1.1.1 kernel: Real Time Clock Driver v1.07
Jun 15 14:28:10 10.1.1.1 kernel: Ramdisk driver initialized : 16 ramdisks of 4096K size
Jun 15 14:28:10 10.1.1.1 kernel: Floppy drive(s): fd0 is 1.44M
```

Fig. 4B

```
Jun 15 14:28:10 10.1.1.1 kernel: FDC 0 is an 8272A
Jun 15 14:28:10 10.1.1.1 kernel: eth0: 3c509 at 0x300 tag 1, 10baseT port, address  00 60 97 97 a3 06, IRQ 9.
Jun 15 14:28:10 10.1.1.1 kernel: 3c509.c:1.12 6/4/97 becker@cesdis.gsfc.nasa.gov
Jun 15 14:28:10 10.1.1.1 kernel: eth1: 3c509 at 0x320 tag 2, 10baseT port, address  00 60 97 a9 c1 42, IRQ 10.
Jun 15 14:28:10 10.1.1.1 kernel: 3c509.c:1.12 6/4/97 becker@cesdis.gsfc.nasa.gov
Jun 15 14:28:10 10.1.1.1 kernel: eth2: 3c509 at 0x340 tag 3, 10baseT port, address  00 60 97 ad c5 2b, IRQ 11.
Jun 15 14:28:10 10.1.1.1 kernel: 3c509.c:1.12 6/4/97 becker@cesdis.gsfc.nasa.gov
Jun 15 14:28:10 10.1.1.1 kernel: VFS: Disk change detected on device 02:00
Jun 15 14:28:10 10.1.1.1 kernel: RAMDISK: Compressed image found at block 440
Jun 15 14:28:10 10.1.1.1 kernel: VFS: Mounted root (minix filesystem) readonly.
Jun 15 14:28:10 10.1.1.1 kernel: WatchGuard Driver v3.00.B120 (C) 1995-1998 WGTI
Jun 15 14:28:10 10.1.1.1 firewalld [48]: new outside interface is eth0
Jun 15 14:28:10 10.1.1.1 firewalld [48]: Starting child /bin/server
Jun 15 14:28:11 10.1.1.1 firewalld [48]: Starting child /opt/bin/tunneld
Jun 15 14:28:11 10.1.1.1 h323 [52]: WatchGuard h323 v3.00.B120 (C) 1998 WGTI
Jun 15 14:28:11 10.1.1.1 sw-proxy [53]: streamworks-proxy launched
Jun 15 14:28:11 10.1.1.1 firewalld [48]: Starting child /opt/bin/webblocker
Jun 15 14:28:11 10.1.1.1 kernel: WG:  reset
Jun 15 14:28:11 10.1.1.1 firewalld [48]: Couldn't find property options.portfwd.hosts, returning ""
Jun 15 14:28:11 10.1.1.1 dce_rpc [54]: WatchGuard dce_rpc v3.00.B120 (C) 1998 WGTI
Jun 15 14:28:12 10.1.1.1 tunneld [56]: WatchGuard PPTP-tunneld v3.00.B120 (C) 1997-1998 WGTI
Jun 15 14:28:12 10.1.1.1 kernel: PPTP: version 1.0.0 (For export)
Jun 15 14:28:12 10.1.1.1 kernel: MPPC: will not compress outgoing packets
Jun 15 14:28:12 10.1.1.1 tunneld [56]: added 1 pptp interfaces
Jun 15 14:28:12 10.1.1.1 tunneld [56]: software compression will not be negotiated
Jun 15 14:28:12 10.1.1.1 nbrecast [60]: WatchGuard NBRecast v3.00.B120 (C) 1998 WGTI
Jun 15 14:28:12 10.1.1.1 tunneld [61]: messenger_init: using syslog as printer (with LOG_WARNING level)
Jun 15 14:28:12 10.1.1.1 tunneld [61]: messenger_init: will read from /tmp/message.61 file
Jun 15 14:28:12 10.1.1.1 firewalld [48]: WatchGuard Daemon, v3.00.B120 (C) 1996-1998 WGTI
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Couldn't connect daytime socket (Connection refused)
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Childmax is 490
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Pid 57, exit status 0
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Pid 56, exit status 0
Jun 15 14:28:12 10.1.1.1 http-proxy [58]: WatchGuard http proxy v3.00.B120 (C) 1996-1998 WGTI
Jun 15 14:28:17 10.1.1.1 authentication [55]: WatchGuard authentication v3.00.B120 (C) 1998 WGTI
Jun 15 14:28:25 10.1.1.1 fwcheck [51]: fwcheck (C) 1998 WGTI
Jun 15 14:28:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:30:08 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:31:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:32:52 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:33:08 10.1.1.1 http-proxy [78]: [10.1.1.15:1094 204.202.129.247:80/java/ScorePost.zip] Response from
   204.202.129.247:80/java/scorepost.zip denied: Unsafe content type "application/zip"
Jun 15 14:33:08 10.1.1.1 http-proxy [79]: [10.1.1.15:1095 204.202.129.247:80/java/starwave/sportszone/scorepost/ScorePost.class]
   Response from 204.202.129.247:80/java/starwave/sportszone/scorepost/scorepost.class denied: Unsafe content type
Jun 15 14:33:08 10.1.1.1 http-proxy [80]: [10.1.1.15:1096 204.202.129.230:80/javanew/lw_ticker/LWScroller.class] Response from
   204.202.129.230:80/javanew/lw_ticker/lwscroller.class denied: Unsafe applet
Jun 15 14:34:21 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:35:42 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:37:01 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:38:22 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:39:51 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:41:17 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:42:30 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:43:45 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:45:10 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:46:38 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:48:00 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:49:28 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:50:42 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:51:58 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:53:11 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:54:36 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:55:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:57:23 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
```

Fig. 4C

Fig. 4D

```
Jun 15 14:57:57 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 63 208.152.24.33 208.152.24.23 3946 113 syn (default)
Jun 15 14:58:35 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:00:04 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:01:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:02:49 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:04:14 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:05:39 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:05:54 10.1.1.1 http-proxy [205]: [10.1.1.15:1144
   208.134.241.152:80/js.ng/Params.richmedia=yes&uniqueID=homepage.main.0&GroupID=400&PagePos=1] Response from
   208.134.241.152:80/js.ng/params.richmedia=yes&uniqueid=homepage.main.0&grou
Jun 15 15:06:10 10.1.1.1 http-proxy [209]: [10.1.1.15:1148
   208.134.241.152:80/js.ng/Params.richmedia=yes&uniqueID=homepage.main.0&GroupID=400&PagePos=1] Response from
   208.134.241.152:80/js.ng/params.richmedia=yes&uniqueid=homepage.main.0&grou
Jun 15 15:06:10 10.1.1.1 http-proxy [210]: [10.1.1.15:1149 208.134.241.155:80/homepage/pics/forecasts_conditions_450.gif] Can't
   send data to client (Broken pipe)
Jun 15 15:06:10 10.1.1.1 http-proxy [208]: [10.1.1.15:1147 208.134.241.155:80/breaking_weather/live_story/pics/hmpg_image.jpg]
   Can't send data to client (Broken pipe)
Jun 15 15:06:10 10.1.1.1 http-proxy [211]: [10.1.1.15:1150 208.134.241.155:80] relaying connection-reset (on read) from client
Jun 15 15:07:06 10.1.1.1 http-proxy [262]: [10.1.1.15:1207 204.133.127.77:80/java/Ticker.class] Response from
   204.133.127.77:80/java/ticker.class denied: Unsafe applet
Jun 15 15:07:08 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:08:35 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:09:50 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:09:59 10.1.1.1 http-proxy [309]: [10.1.1.17:1074 206.35.113.28:80/F/OCVscroll.class] Response from
   206.35.113.28:80/f/ocvscroll.class denied: Unsafe content type "application/octet-stream"
Jun 15 15:10:00 10.1.1.1 http-proxy [310]: [10.1.1.17:1075 206.35.113.28:80/F/resbar.gif] Can't send data to client (Broken pipe)
Jun 15 15:10:00 10.1.1.1 http-proxy [311]: [10.1.1.17:1076 206.35.113.28:80/F/331.gif] Can't send data to client (Broken pipe)
Jun 15 15:10:00 10.1.1.1 http-proxy [312]: [10.1.1.17:1077 206.35.113.28:80/F/copyrigh.gif] Can't send data to client (Broken pipe)
Jun 15 15:10:00 10.1.1.1 http-proxy [313]: [10.1.1.17:1078 206.35.113.28:80] relaying connection-reset (on read) from client
Jun 15 15:11:03 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:12:19 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:13:32 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:13:53 10.1.1.1 http-proxy [336]: [10.1.1.21:1034 206.69.91.100:80/neonews/Scroll.class] Response from
    206.69.91.100:80/neonews/scroll.class denied: Unsafe applet
Jun 15 15:14:21 10.1.1.1 http-proxy [349]: [10.1.1.21:1048 141.142.3.70:80/java/mamagator.class] Response from
    141.142.3.70:80/java/mamagator.class denied: Unsafe content type "application/octet-stream"
Jun 15 15:14:54 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:16:12 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:17:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:18:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:19:58 10.1.1.1 http-proxy [382]: [10.1.1.19:1027 207.25.71.22:80/virtual/1998/code/cnn.js] Response from
    207.25.71.22:80/virtual/1998/code/cnn.js denied: Unsafe content type "application/x-javascript"
Jun 15 15:20:11 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:20:28 10.1.1.1 http-proxy [393]: [10.1.1.19:1041 204.152.178.145:80/phrack52.tar.gz] Response from
    204.152.178.145:80/phrack52.tar.gz denied: Unsafe content type "application/x-tar"
Jun 15 15:21:37 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:22:52 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:24:12 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:25:36 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:27:03 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:28:21 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:29:37 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:30:51 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:31:03 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 63 208.152.24.33 208.152.24.23 4124 113 syn (default)
Jun 15 15:32:20 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:33:33 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:34:48 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:36:02 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:37:21 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:37:39 10.1.1.1 firewalld [48]: deny in eth0 56 icmp 20 255 208.152.24.30 208.152.24.23 5 1 (default)
Jun 15 15:38:44 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:40:00 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:41:22 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:41:55 10.1.1.1 http-proxy [585]: [10.1.1.20:1029 192.215.74.11:80] relaying connection-reset (on read) from client
```

Fig. 4E

```
Jun 15 15:42:45 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:44:10 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:45:33 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:46:43 10.1.1.1 http-proxy [610]: [10.1.1.25:1030 209.67.29.11:80/java/NewsTicker/NewsTicker1.class] Response from
    209.67.29.11:80/java/newsticker/newsticker1.class denied: Unsafe applet
Jun 15 15:46:48 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:46:54 10.1.1.1 http-proxy [617]: [10.1.1.25:1037 209.67.29.11:80] relaying connection-reset (on read) from client
Jun 15 15:46:55 10.1.1.1 http-proxy [627]: [10.1.1.25:1047 209.67.29.11:80] relaying connection-reset (on read) from client
Jun 15 15:48:09 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:49:34 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:51:03 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:52:04 10.1.1.1 http-proxy [670]: [10.1.1.30:1061 206.99.97.11:80] connection timed out: exiting
Jun 15 15:52:18 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:53:31 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:54:36 10.1.1.1 http-proxy [704]: [10.1.1.30:1096 206.99.97.11:80] connection timed out: exiting
Jun 15 15:54:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:56:19 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:57:46 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:59:09 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:00:24 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:01:42 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:03:01 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:04:22 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:04:25 10.1.1.1 http-proxy [763]: [10.1.1.24:1047 168.100.205.221:80] relaying connection-reset (on read) from client
Jun 15 16:05:39 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:07:08 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:08:31 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:09:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1024 4102 syn (default)
Jun 15 16:09:25 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1024 4102 syn (default)
Jun 15 16:09:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1030 4102 syn (default)
Jun 15 16:09:55 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:10:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1031 4102 syn (default)
```

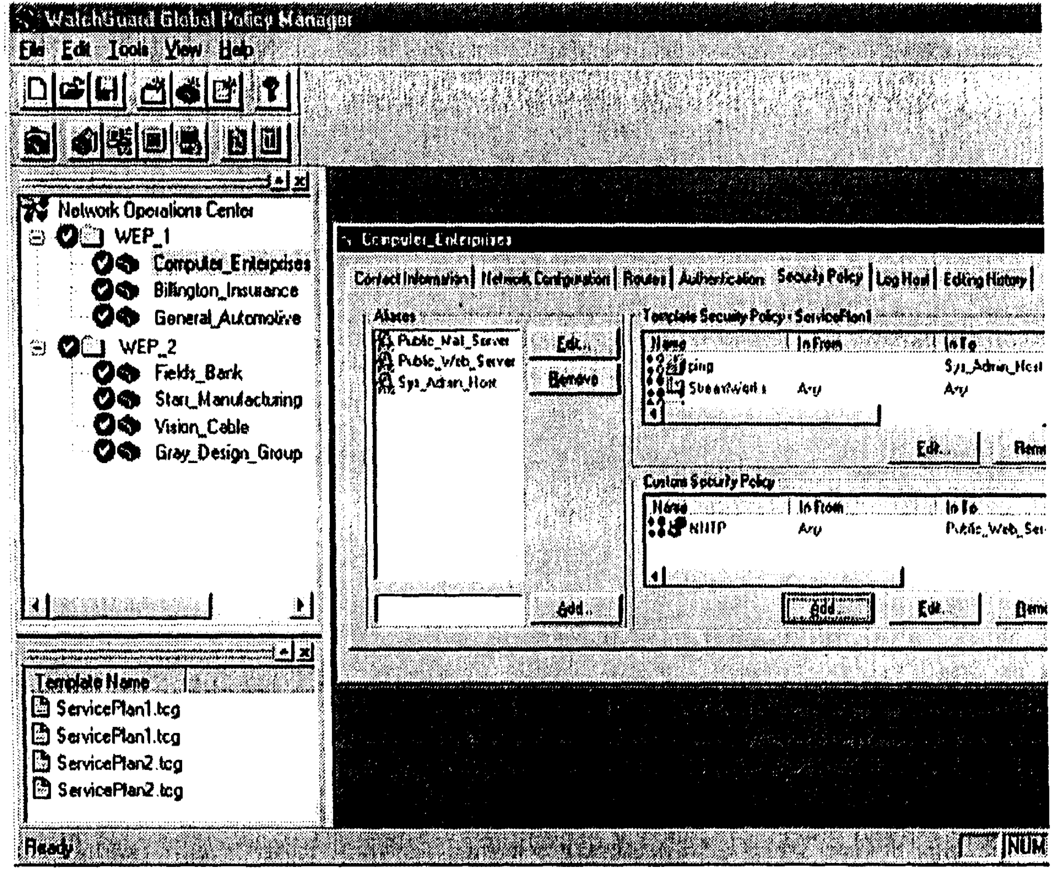
Fig. 4F

```
Jun 15 16:10:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1037 4102 syn (default)
Jun 15 16:11:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1090 4102 syn (default)
Jun 15 16:11:25 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:11:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1095 4102 syn (default)
Jun 15 16:12:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1096 4102 syn (default)
Jun 15 16:12:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1152 4102 syn (default)
Jun 15 16:12:55 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:13:08 10.1.1.1 http-proxy [825]: [10.1.1.23:1042 204.202.129.247:80/java/ScorePost.zip] Response from
    204.202.129.247:80/java/scorepost.zip denied: Unsafe content type "application/zip"
Jun 15 16:13:09 10.1.1.1 http-proxy [826]: [10.1.1.23:1043 204.202.129.247:80/java/starwave/sportszone/scorepost/ScorePost.class]
    Response from 204.202.129.247:80/java/starwave/sportszone/scorepost/scorepost.class denied: Unsafe content type
Jun 15 16:13:09 10.1.1.1 http-proxy [827]: [10.1.1.23:1044 204.202.129.230:80/javanew/lw_ticker/LWScroller.class] Response from
    204.202.129.230:80/javanew/lw_ticker/lwscroller.class denied: Unsafe applet
Jun 15 16:13:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1216 4102 syn (default)
Jun 15 16:13:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1283 4102 syn (default)
Jun 15 16:14:20 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:14:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1284 4102 syn (default)
Jun 15 16:14:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1285 4102 syn (default)
Jun 15 16:15:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1286 4102 syn (default)
Jun 15 16:15:37 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:15:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1287 4102 syn (default)
Jun 15 16:16:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1288 4102 syn (default)
Jun 15 16:16:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1294 4102 syn (default)
Jun 15 16:17:02 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:17:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1297 4102 syn (default)
Jun 15 16:17:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1298 4102 syn (default)
Jun 15 16:18:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1361 4102 syn (default)
Jun 15 16:18:31 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:18:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1362 4102 syn (default)
Jun 15 16:19:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1424 4102 syn (default)
Jun 15 16:19:49 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:19:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1488 4102 syn (default)
```

Fig. 4G

```
Jun 15 16:20:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1559 4102 syn (default)
Jun 15 16:20:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1563 4102 syn (default)
Jun 15 16:21:04 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:21:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1564 4102 syn (default)
Jun 15 16:21:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1565 4102 syn (default)
Jun 15 16:22:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1567 4102 syn (default)
Jun 15 16:22:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:22:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1569 4102 syn (default)
Jun 15 16:23:53  controld: Error: Connection reset by peer. Receive:  error #10054
Jun 15 16:23:57  controld: WatchGuard controld 3.00.B120 (C) 1996-1998 Watchguard Technologies
Jun 11 02:43:58 198.245.206.12 firewalld [49]: deny in eth1 242 udp 20 32 198.245.206.208 198.245.206.255 138 138 (SMB)
Jun 15 16:24:13  controld: WatchGuard controld 3.00.B120 (C) 1996-1998 Watchguard Technologies
```

Fig. 4H


WatchGuard Global Policy Manager
File Edit Tools View Help
Computer_Enterprises
Contact Information | Network Configuration | Routes | Authorization | Security Policy | Log Host | Editing History
Aliases
Edit...
Remove
Add...
Edit...
Rem
Add...
Edit...
Rem
Ready
NUM

Network Operations Center
- WEP_1
  - Computer_Enterprises
  - Billington_Insurance
  - General_Automotive
- WEP_2
  - Fields_Bank
  - Starr_Manufacturing
  - Vision_Cable
  - Gray_Design_Group

Template Name
ServicePlan1.tcg
ServicePlan1.tcg
ServicePlan2.tcg
ServicePlan2.tcg

Aliases

- Public_Mail_Server
- Public_Web_Server
- Sys_Admin_Host

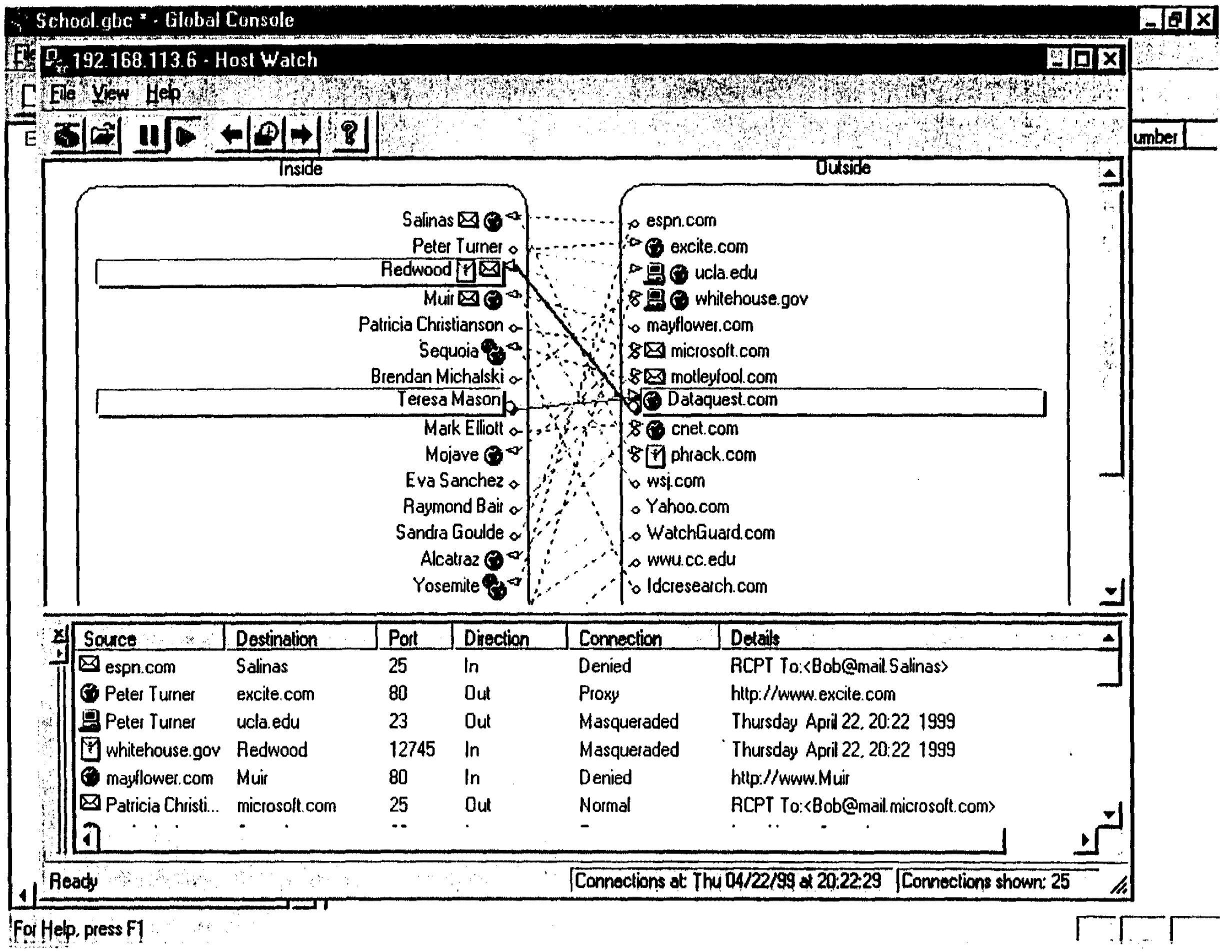
Template Security Policy : ServicePlan1

Name	In From	In To
ping		Sys_Admin_Host
StreamWorks	Any	Any

Custom Security Policy

Name	In From	In To
NNTP	Any	Public_Web_Ser

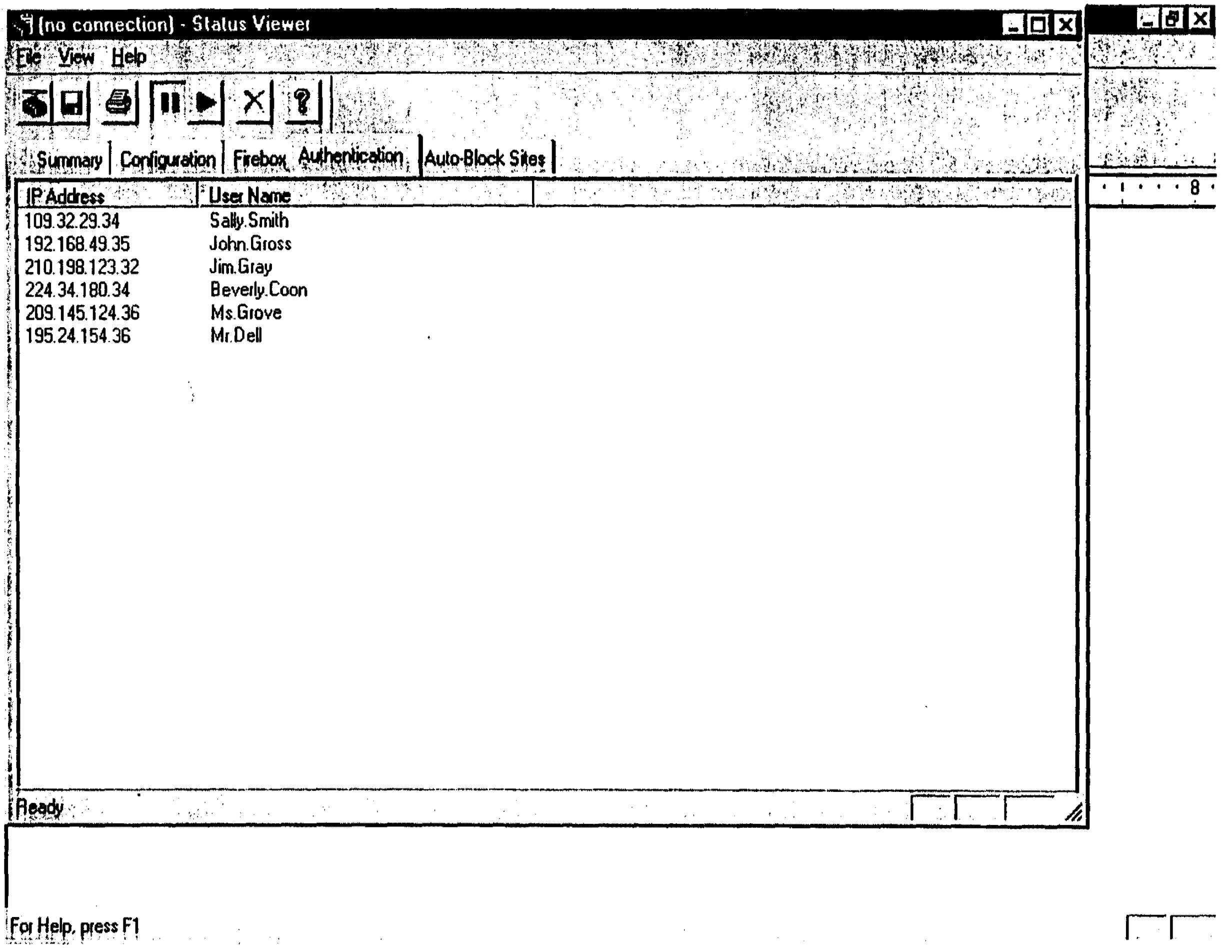
Fig. 5A



Source	Destination	Port	Direction	Connection	Details
☒ espn.com	Salinas	25	In	Denied	RCPT To:<Bob@mail.Salinas>
● Peter Turner	excite.com	80	Out	Proxy	http://www.excite.com
Peter Turner	ucla.edu	23	Out	Masqueraded	Thursday April 22, 20:22 1999
whitehouse.gov	Redwood	12745	In	Masqueraded	Thursday April 22, 20:22 1999
● mayflower.com	Muir	80	In	Denied	http://www.Muir
☒ Patricia Christi...	microsoft.com	25	Out	Normal	RCPT To:<Bob@mail.microsoft.com>

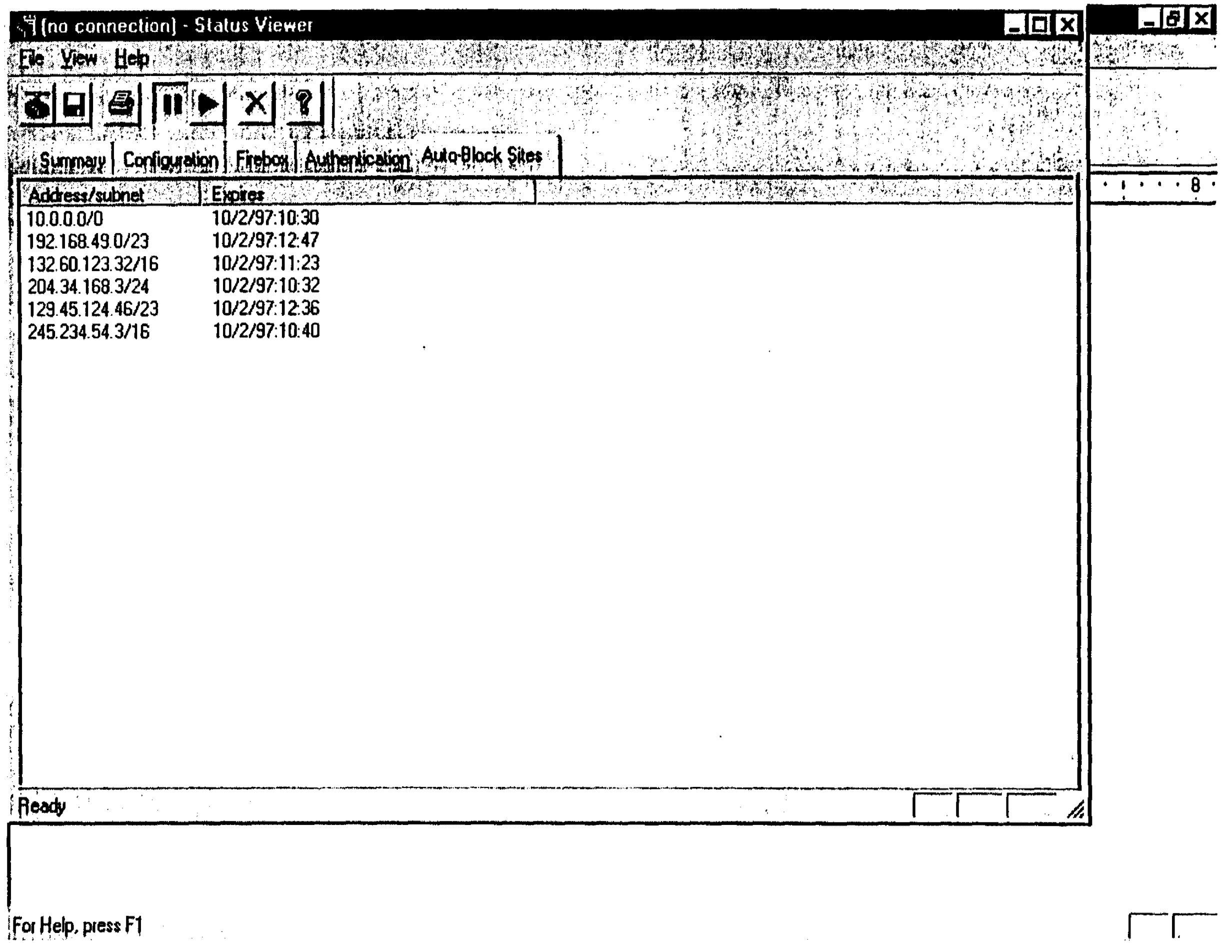
Ready | Connections at: Thu 04/22/99 at 20:22:29 | Connections shown: 25

Fig. 5B



IP Address	User Name
109.32.29.34	Sally.Smith
192.168.49.35	John.Gross
210.198.123.32	Jim.Gray
224.34.180.34	Beverly.Coon
209.145.124.36	Ms.Grove
195.24.154.36	Mr.Dell

Fig. 5C

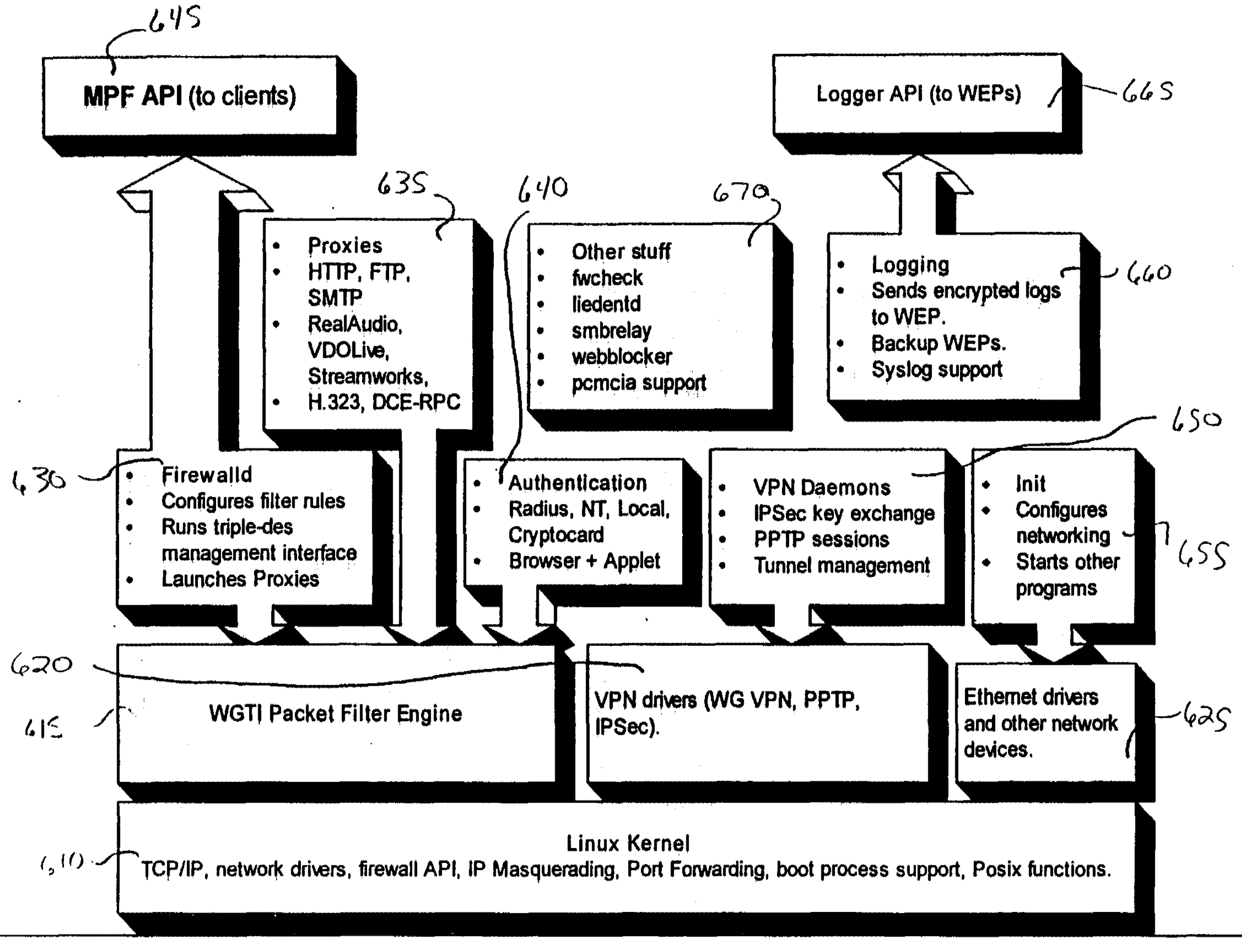


Address/subnet	Expires
10.0.0.0/0	10/2/97:10:30
192.168.49.0/23	10/2/97:12:47
132.60.123.32/16	10/2/97:11:23
204.34.168.3/24	10/2/97:10:32
129.45.124.46/23	10/2/97:12:36
245.234.54.3/16	10/2/97:10:40

Fig. 5D.

Fig. 6

Appliance Architecture



- Proxies
- HTTP, FTP, SMTP
- RealAudio, VDOLive, Streamworks,
- H.323, DCE-RPC

- Other stuff
- fwcheck
- liedentd
- smbrelay
- webblocker
- pcmcia support

- Logging
- Sends encrypted logs to WEP.
- Backup WEPs.
- Syslog support

- Firewalld
- Configures filter rules
- Runs triple-des management interface
- Launches Proxies

- Authentication
- Radius, NT, Local, Cryptocard
- Browser + Applet

- VPN Daemons
- IPSec key exchange
- PPTP sessions
- Tunnel management

- Init
- Configures networking
- Starts other programs

WGTI Packet Filter Engine

VPN drivers (WG VPN, PPTP, IPSec).

Ethernet drivers and other network devices.

Linux Kernel

TCP/IP, network drivers, firewall API, IP Masquerading, Port Forwarding, boot process support, Posix functions.

Fig. 7

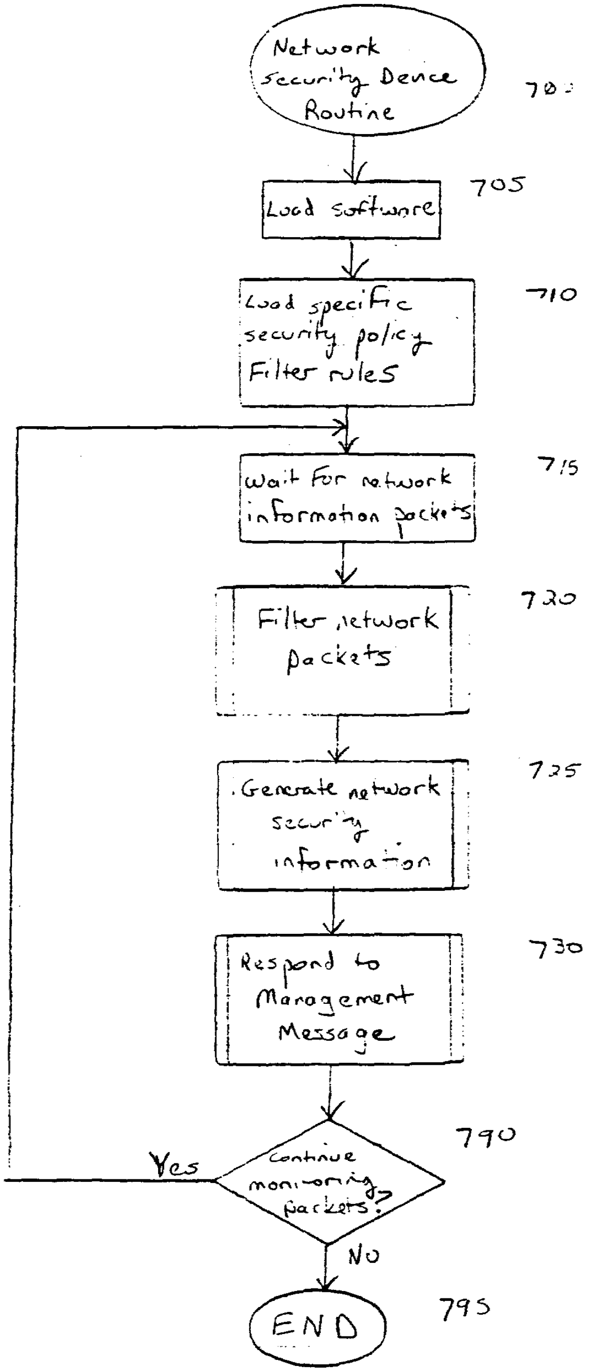

Network Security Device Routine
700
Load software
705
Load specific security policy Filter rules
710
Wait for network information packets
715
Filter network packets
720
Generate network security information
725
Respond to Management Message
730
Continue monitoring packets?
790
Yes
No
END
795

Fig. 8

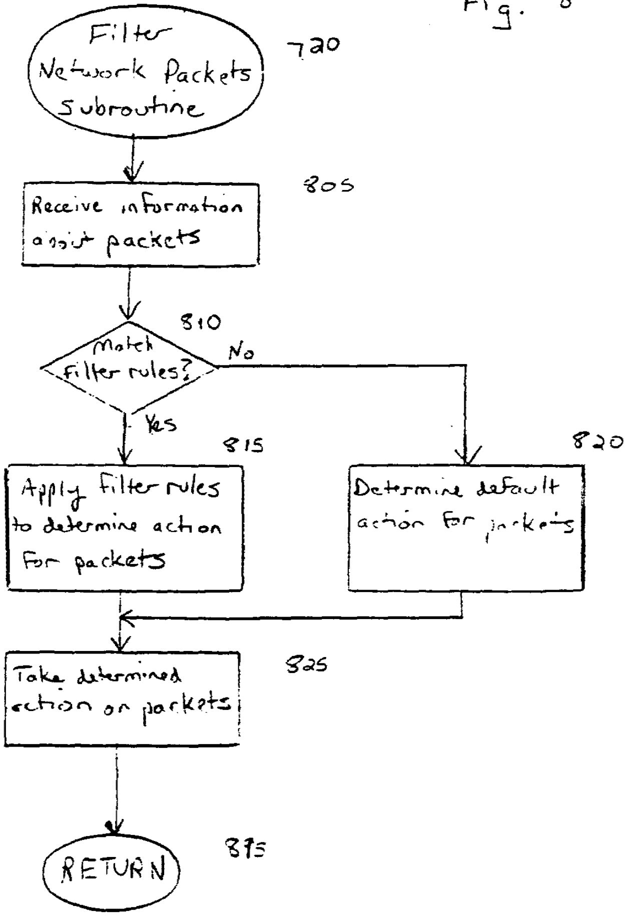
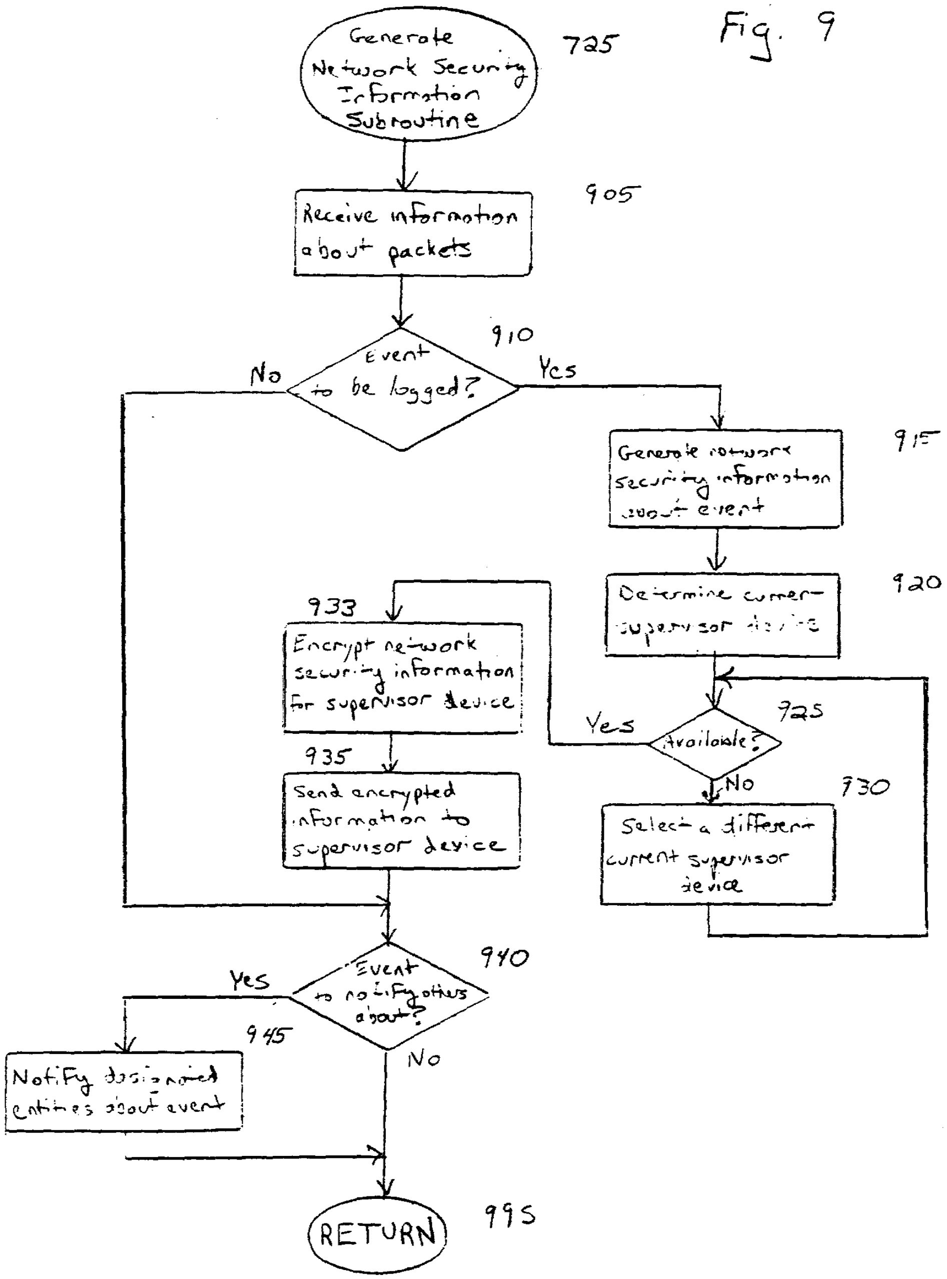

Filter Network Packets Subroutine
720
805
Receive information about packets
810
Match filter rules?
No
Yes
815
Apply filter rules to determine action for packets
820
Determine default action for packets
825
Take determined action on packets
875
RETURN

Fig. 9


Generate Network Security Information Subroutine
725
Receive information about packets
905
Event to be logged?
910
No
Yes
Generate network security information about event
915
Determine current supervisor device
920
Available?
725
Yes
No
Select a different current supervisor device
730
Encrypt network security information for supervisor device
933
Send encrypted information to supervisor device
935
Event to notify others about?
940
Yes
No
Notify designated entities about event
945
RETURN
995

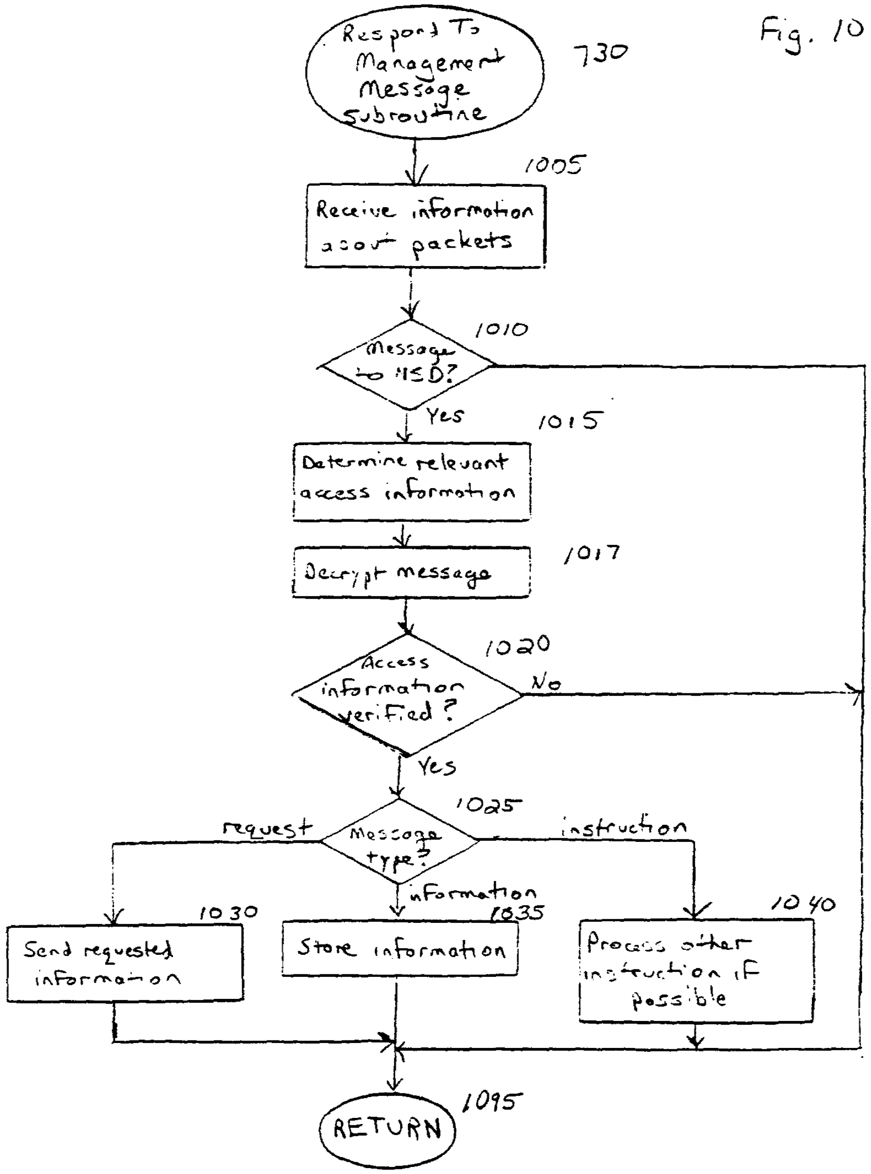


Fig. 10
Respond To Management Message Subroutine
730
1005
Receive information about packets
1010
Message to MSD?
Yes
1015
Determine relevant access information
1017
Decrypt message
1020
Access information verified?
No
Yes
1025
Message type?
request
instruction
information
1030
Send requested information
1035
Store information
1040
Process other instruction if possible
1095
RETURN

Fig. 11

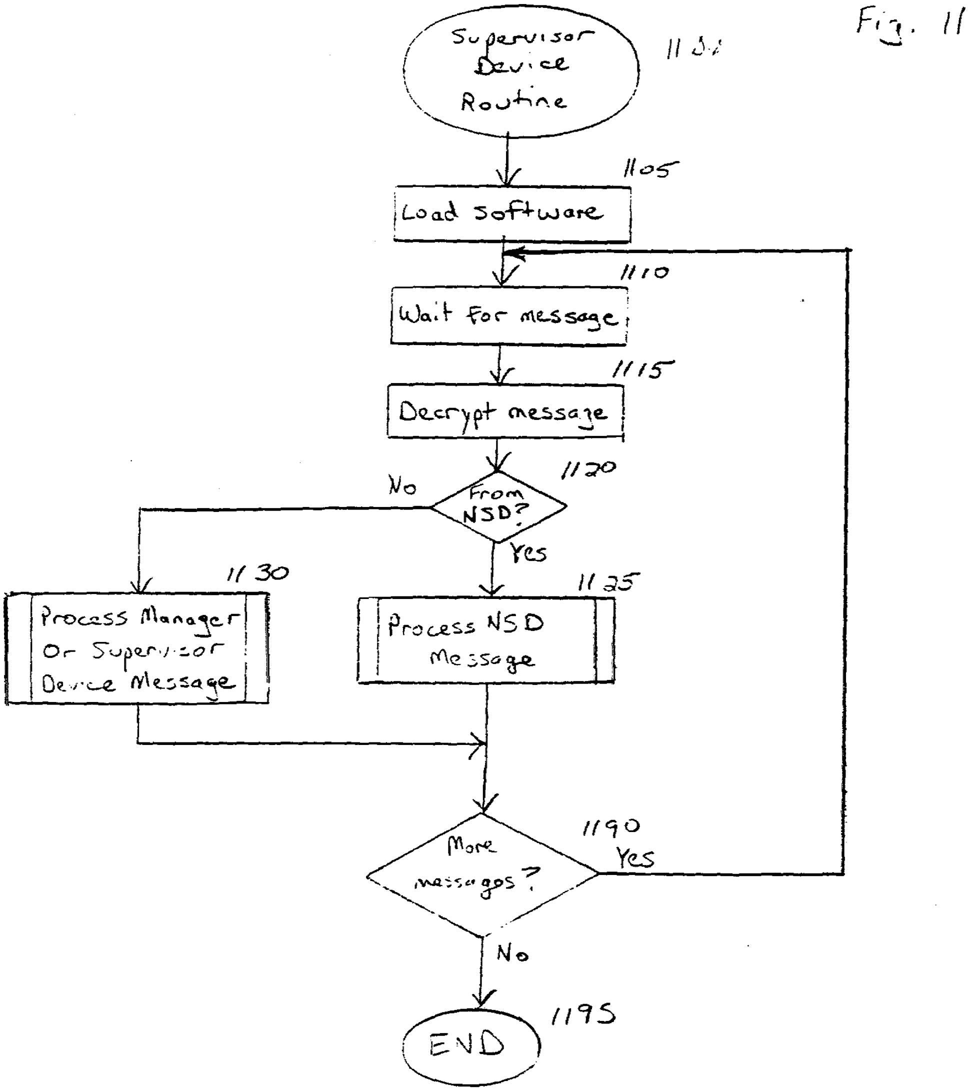

Supervisor Device Routine
1100
Load software
1105
Wait for message
1110
Decrypt message
1115
From NSD?
1120
No
Yes
Process Manager Or Supervisor Device Message
1130
Process NSD Message
1125
More messages?
1190
Yes
No
END
1195

Fig. 12

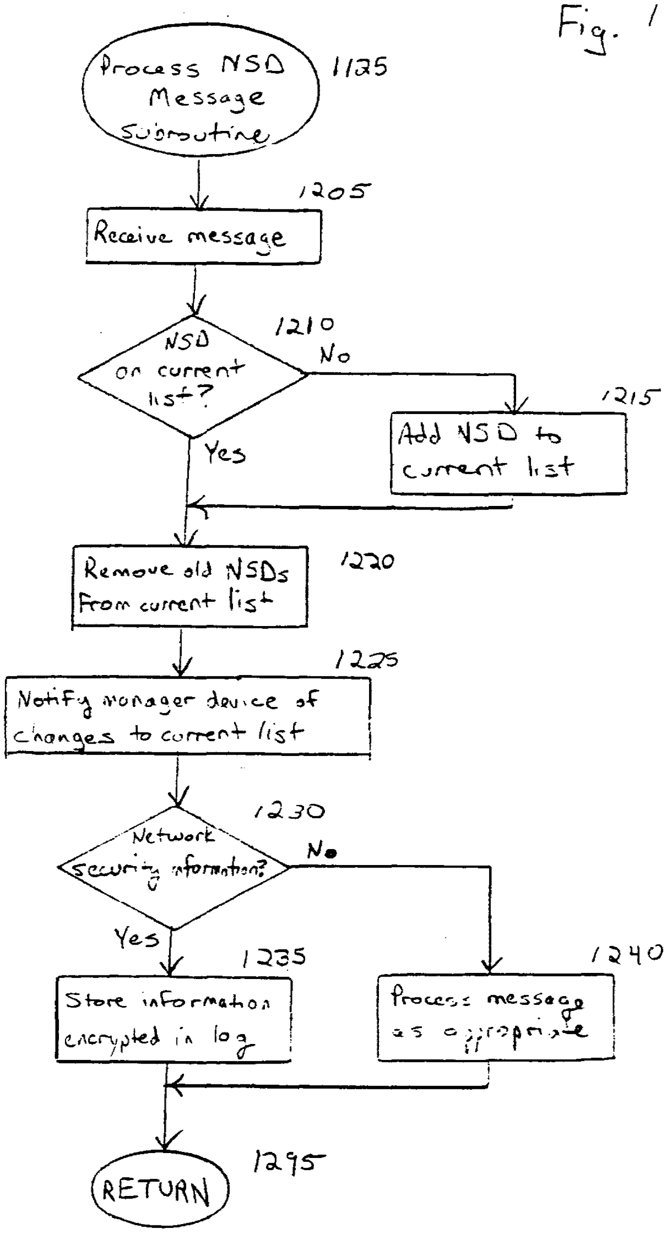

Process NSD Message Subroutine
1125
1205
Receive message
1210
NSD on current list?
No
1215
Add NSD to current list
Yes
Remove old NSDs From current list
1220
1225
Notify manager device of changes to current list
1230
Network security information?
No
Yes
1235
Store information encrypted in log
1240
Process message as appropriate
1295
RETURN

Fig. 13

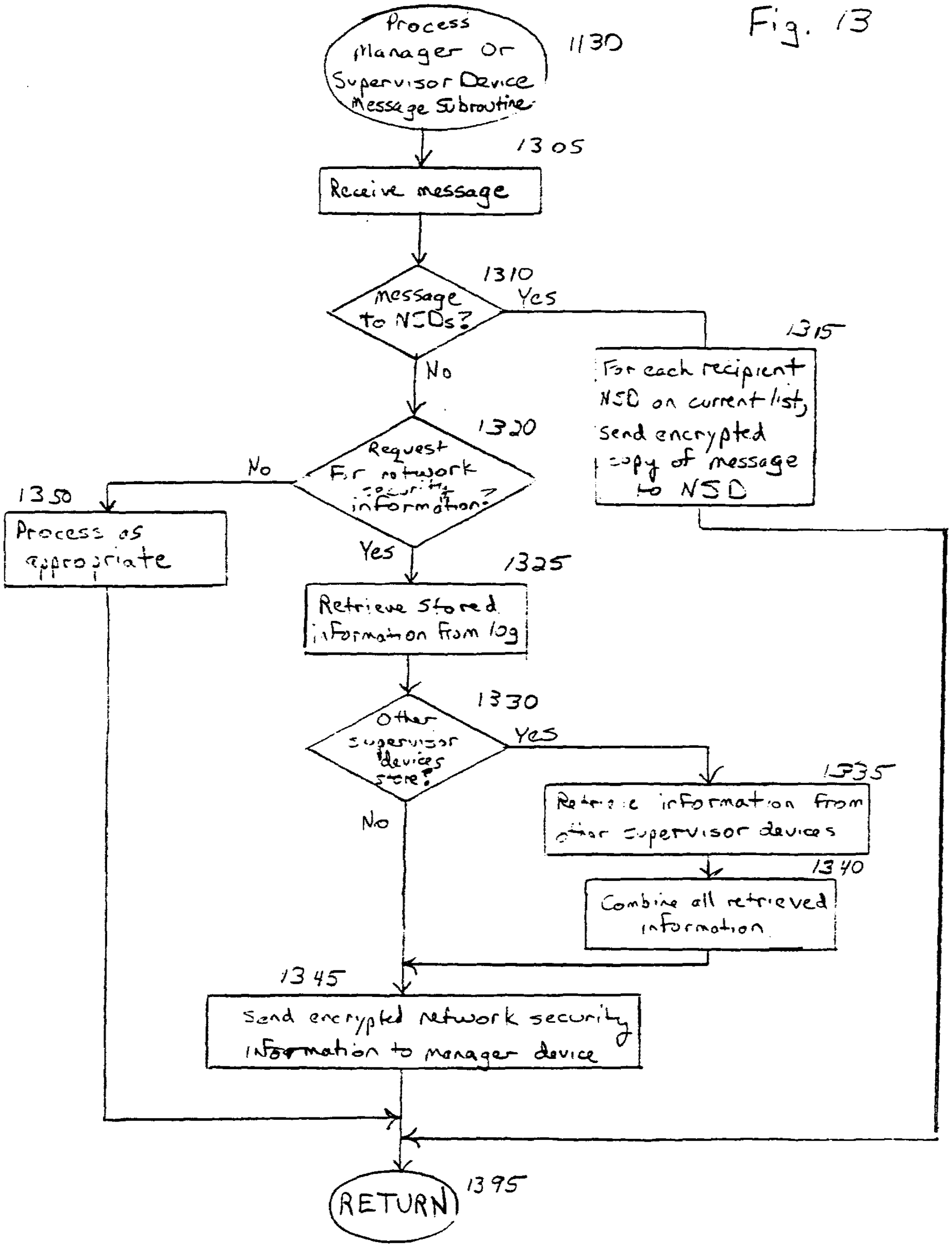

Process Manager Or Supervisor Device Message Subroutine
1130
1305
Receive message
1310
message to NSDs?
Yes
1315
For each recipient NSD on current list, send encrypted copy of message to NSD
No
1320
Request for network security information?
No
1350
Process as appropriate
Yes
1325
Retrieve stored information from log
1330
Other supervisor devices store?
Yes
1335
Retrieve information from other supervisor devices
1340
Combine all retrieved information
No
1345
Send encrypted network security information to manager device
1395
RETURN

Fig. 14A

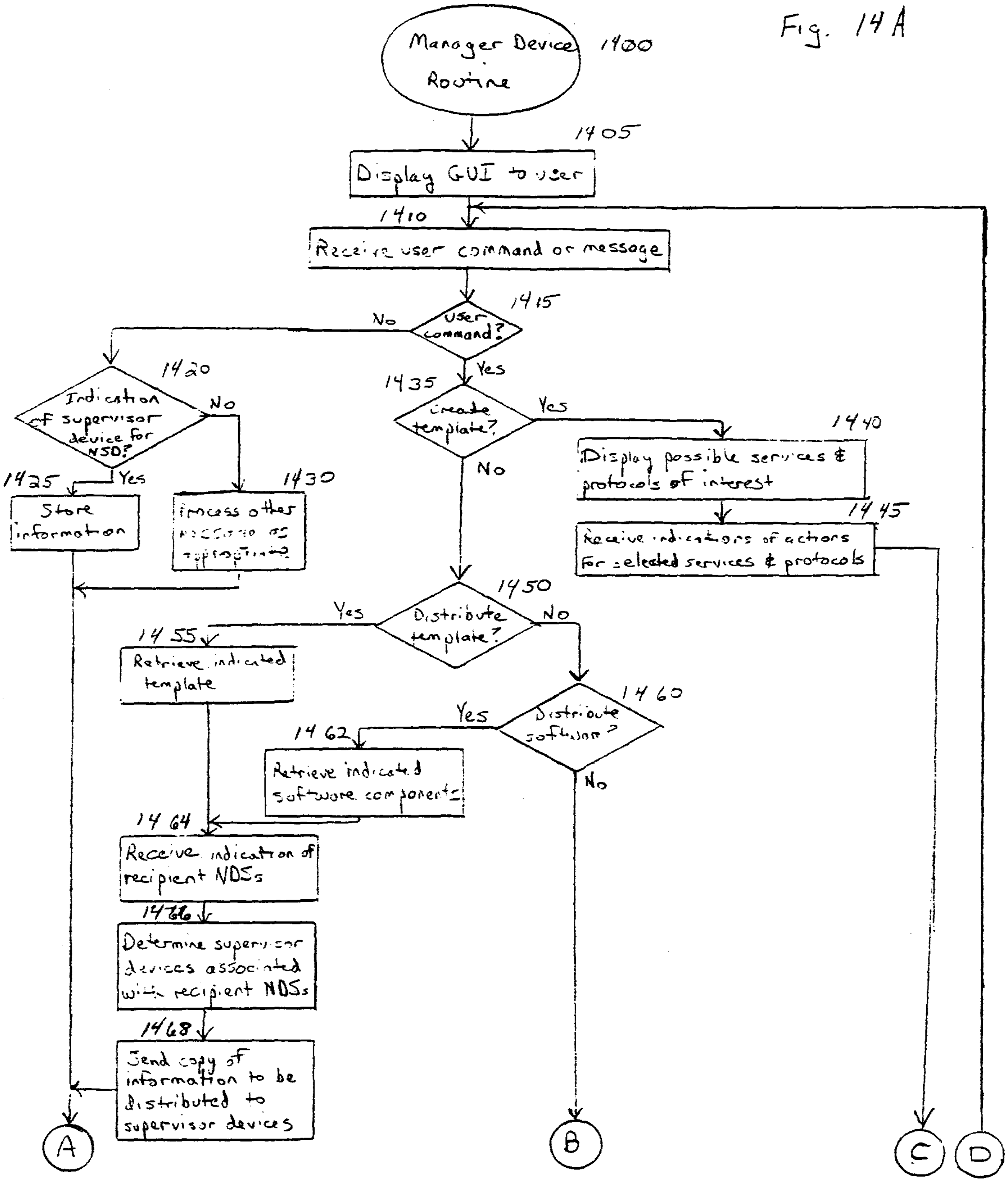
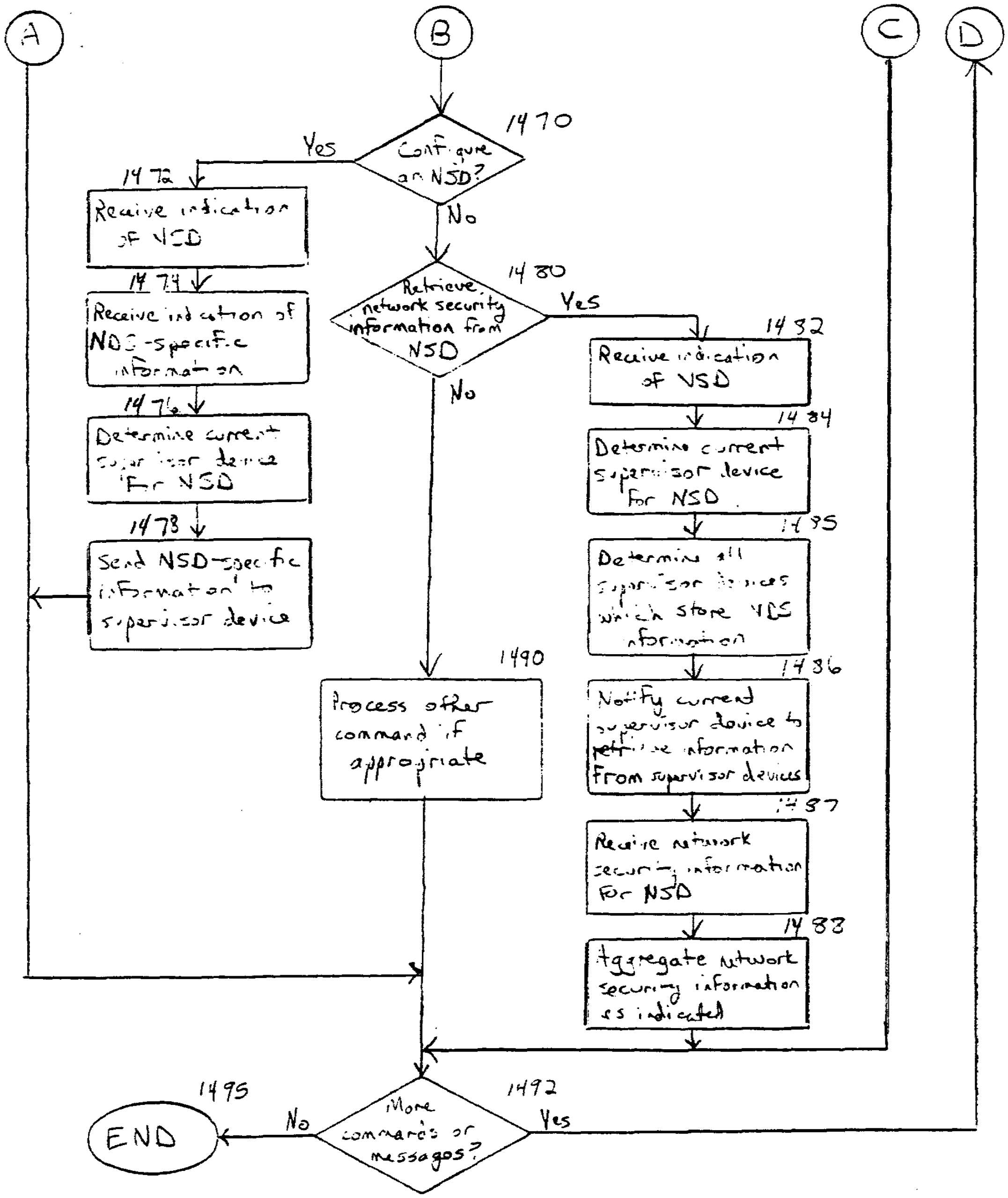

Manager Device Routine
1400
1405
Display GUI to user
1410
Receive user command or message
1415
User command?
No
Yes
1420
Indication of supervisor device for NSD?
No
Yes
1425
Store information
1430
Process other messages as appropriate
1435
Create template?
Yes
No
1440
Display possible services & protocols of interest
1445
Receive indications of actions for selected services & protocols
1450
Distribute template?
Yes
No
1455
Retrieve indicated template
1460
Distribute software?
Yes
No
1462
Retrieve indicated software components
1464
Receive indication of recipient NDSs
1466
Determine supervisor devices associated with recipient NDSs
1468
Send copy of information to be distributed to supervisor devices
A
B
C
D

Fig. 14 B


A
B
C
D
1470
Configure an NSD?
Yes
No
1472
Receive indication of NSD
1474
Receive indication of NDS-specific information
1476
Determine current supervisor device for NSD
1478
Send NSD-specific information to supervisor device
1480
Retrieve network security information from NSD
Yes
No
1482
Receive indication of NSD
1484
Determine current supervisor device for NSD
1485
Determine all supervisor devices which store NDS information
1486
Notify current supervisor device to ~~ret~~rieve information from supervisor devices
1487
Receive network security information for NSD
1488
Aggregate network security information as indicated
1490
Process other command if appropriate
1492
More commands or messages?
Yes
No
1495
END

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/US 00/09942

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/24 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 54644 A (3COM CORP) 3 December 1998 (1998-12-03) abstract figure 1 page 1, line 5 - line 19 page 5, line 5 -page 6, line 17 page 28, line 20 -page 30, line 30 ---	1,77,88, 102
E	US 6 052 728 A (TERADA MASATO ET AL) 18 April 2000 (2000-04-18) abstract column 1, line 35 - line 59 column 2, line 1 - line 39 column 15, line 1 - line 42 --- -/--	1,77,88, 102

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 August 2000	Date of mailing of the international search report 04/09/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Adkhis, F

Interı   nal Application No
PCT/US 00/09942

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 577 209 A (BOYLE JOHN M ET AL) 19 November 1996 (1996-11-19) abstract column 2, line 38 - line 44 column 4, line 18 - line 53 -----	1-105

1

INTERNATIONAL SEARCH REPORT

. ıormation on patent family members

Interr nal Application No
PCT/US 00/09942

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
WO 9854644	A	03-12-1998	US	5968176	A	19-10-1999
			EP	0990206	A	05-04-2000
			GB	2342020	A	29-03-2000
US 6052728	A	18-04-2000	JP	10198616	A	31-07-1998
US 5577209	A	19-11-1996	US	5940591	A	17-08-1999

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
BORDEN LADNER GERVAIS LLP
World Exchange Plaza
1100 - 100 Queen Street
OTTAWA, Ontario
Canada, K1P 1J9

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* 20 June 2005 (20-06-2005)

Applicant's or agent's file reference
PAT58913W-90

FOR FURTHER ACTION
See paragraph 2 below

International application No. **PCT/CA2005/000294**	International filing date *(day/month/year)* 25 February 2005 (25-02-2005)	Priority date *(day/month/year)* 04 April 2004 (04-04-2004)

International Patent Classification (IPC) or both national classification and IPC
IPC(7): H04L 9/00

Applicant
RESEARCH IN MOTION LIMITED

1. This opinion contains indications relating to the following items :

[X]	Box No. I	Basis of the opinion
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[X]	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**
If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Date of completion of this opinion 08 June 2005 (08-06-2005)	Authorized officer Jamie Hayami (819) 934-2670

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [X] the international application in the language in which it was filed

   [ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of :

   a. type of material

      [ ] a sequence listing

      [ ] table(s) related to the sequence listing

   b. format of material

      [ ] on paper

      [ ] in electronic form

   c. time of filing/furnishing

      [ ] contained in the international application as filed.

      [ ] filed together with the international application in electronic form

      [ ] furnished subsequently to this Authority for the purposes of search.

3 [ ] In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statement that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments :

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-7, 9-14, 16-19, 22	YES
	Claims	8, 15, 20, 21	NO
Inventive step (IS)	Claims	1-7, 9-14, 16-19, 22	YES
	Claims	8, 15, 20, 21	NO
Industrial applicability (IA)	Claims	1-22	YES
	Claims	None	NO

2. Citations and explanations :

The claimed invention relates to a method and system for establishing a security-related mode of operation for computing devices.

This opinion is formed based on the originally filed claims 1-22.

The following relevant document appears in the International Search Report:

D1: WO 00/69120 A1

D1 discloses a facility for using a security policy manager device to remotely manage multiple network security devices (NSDs). The system allows a manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information. The system also allows a manager device to retrieve, analyze and display all of the network security information gathered by the various NSDs while implementing security policies.

Novelty (N)

Claims 8, 15, 20, and 21 do not comply with **PCT Article 33(2)**. D1disclosed the claimed subject matter before the claim date.

In regards to independent claim 8, D1 discloses: a computing device utilizing a centralized policy data store to implement a security-related mode of operation (see D1: page 5, lines 1-6, "*the facility allows the manager device to create a consistent security policy for the multiple NSDs by distributing a security policy template ...* "), the device comprising:

- a communication interface configured to facilitate communication between the centralized policy data store and the computing device (see D1, page 9, lines 16-22, "*the Network Security Device Management System includes a security policy manager device able to communicate with multiple supervisor devices ...*"); and
- a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (see D1, page 9, lines 16-22, "*the Network Security Device Management System includes a security policy manager device able to communicate with multiple supervisor devices ...*");
- wherein the processing instructions includes security instructions configured to place the computing device in a secure mode of operation responsive to configuration data received from the centralized policy data store via the communication interface (see D1, page 6, line 1 to page 7, line 1; page 7, lines 20-26; page 8, lines 13-19; and page 11, lines 4-24).

Therefore claim 8 is not novel in view of D1and does not comply with **PCT Article 33(2)**.

(See Supplemental Box)

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made :

Drawings

The description does not comply with **PCT Rule 11.13(l)**. Reference signs not mentioned in the description shall not appear in the drawings, and vice versa. Reference numerals 25 (figures 1 and 2), 70 (figure 2), 115 (figure 2), and 500 (figure 7) are shown in the drawings, however they do not appear in the description.

The drawings do not comply with **PCT Rule 11.13(l)**. The same features, when denoted by reference signs, shall, throughout the entire application, be denoted by the same signs. In figure 2, reference numeral 100 is used to denote a mobile data communication device as well as a connection between wireless VPN router and wireless network 1.

Description Informalities

The description does not comply with **PCT Article 5**. A statement in an application, such as found on page 5, lines 27-28 which incorporates by reference any other document, does not comply with PCT Article 5. The description should be complete in and of itself. A person skilled in the art should be able to understand the patent specification without reference to any other document.

Indefiniteness

Claims 6, 9 and 11 are unclear and do not comply with **PCT Article 6**. The following terms "the use" (claim 6, line 16), "the devices" (claim 6, line 17) and "the device's user" (claim 9, line 2; claim 11, lines 9-10) lack a proper antecedent basis.

Claims 6 and 11 are unclear and do not comply with **PCT Article 6**. The double inclusion of any element renders the claims indefinite. The terms "a plurality of computing devices" (claim 6, line 6), "an administrator" (claim 6, line 14), "a security mode of operation" (claim 6, lines 14-15), and "a visual indication" (claim 11, line 9) have already been defined previously in the claims. The aforementioned terms should therefore be referred to using a definite article.

Claim 7 is indefinite and does not comply with **PCT Article 6**. The inclusion of "and combinations thereof' causes ambiguity.

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of: V

Independent claims 15, 20 and 21 contain the same combination of features as found in independent claim 1, in the form of method, digital signal and computer software claims. Therefore, the subject matter of claims 15, 20 and 21 are not novel in view of D1and do not comply with **PCT Article 33(2)**.

Claims 1-7, 9-14, 16-19 and 22 are novel and do comply with **PCT Article 33(2)** as D1 does not disclose explicitly the features of a security mode data structure contained within a policy data store; wherein computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, the output being configured to comprise a visual indication of the security mode of operation to the device's user. D1 also does not disclose that the secure mode of operation comprises a Federal Information Processing Standard mode of operation; a first security mode data structure includes a first security mode being associated with a first plurality of computing device and a second security mode data structure includes a second security mode being associated with a second plurality of computing devices; and that the sending of the stored security mode of operation forces use of Advanced Encryption Standard or Triple Data Encryption Standard.

Inventive Step (IS)

Claims 8, 15, 20 and 21 do not comply with **PCT Article 33(3)** as they do not define any new matter beyond the teaching of D1, and therefore cannot be viewed as involving an inventive step (see above arguments with respect to novelty).

Claims 1-7, 9-14, 16-19 and 22 comply with **PCT Article 33(3)**. The subject matter of claims 1-7, 9-14, 16-19 and 22 are considered to involve an inventive step since, having regard to the prior art, they are not obvious to a person skilled in the art.

Industrial Applicability (IA)

The subject matter of claims 1-22 are considered to be industrially applicable and thus fulfill the requirements of **PCT Article 33(4)**.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PAT58913W-90	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. **PCT/CA2005/000294**	International filing date *(day/month/year)* 25 February 2005 (25-02-2005)	(Earliest)Priority date *(day/month/year)* 04 April 2004 (04-04-2004)
Applicant RESEARCH IN MOTION LIMITED		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

[X] the international application in the language in which it was filed

[ ] a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I

2. [ ] **Certain claims were found unsearchable** (see Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No. III)

4. With regard to the **title**,

[X] the text is approved as submitted by the applicant

[ ] the text has been established by this Authority to read as follows :

5. With regard to the **abstract**,

[X] the text is approved as submitted by the applicant

[ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 6

[X] as suggested by the applicant

[ ] as selected by this Authority, because the applicant failed to suggest a figure

[ ] as selected by this Authority, because this figure better characterizes the invention

b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000294

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7): H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(7): H04L 9/00, H04L*

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Canadian Patent Database, Delphion, Google. Keywords: security mode, operation, policy data store, configure devices, security policy, mobile, display, FIPS.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/69120 A1 (ROTHERMEL ET AL.) 16 November 2000 (16-11-2000)	8, 15, 20, 21
A	page 4, line 23 to page 5, line 18	1, 4, 5, 6, 7, 22
	page 6, line 23 to page 11, line 27	
	page 16, lines 10-17	
	page 17, lines 14-20	
A	US 6,202,157 B1 (BROWNLIE ET AL.) 13 March 2001 (13-03-2001) column 2, line 56 to column 3, line 34 column 3, lines 50-58 column 4, line 61 to column 5, line 5	1, 4, 5, 6, 7, 8, 15, 20, 21, 22
A, P	US 6,732,168 B1 (BEARDEN ET AL.) 4 May 2004 (04-05-2004) column 2, lines 6-48 column 3, line 62 to column 4, line 13 column 5, line 45 to column 6, line 9 column 6, lines 25-64	1, 4, 5, 6, 7, 8, 15, 20, 21, 22

[ ] Further documents are listed in the continuation of Box C. [X] See patent family annex.

*	Special categories of cited documents :	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier application or patent but published on or after the international filing date		
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 30 May 2005 (30-05-2005)	Date of mailing of the international search report 20 June 2005 (20-06-2005)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Jamie Hayami (819) 934-2670

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2005/000294

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO0069120	16-11-2000	AU4346600 A EP1175752 A1 JP2002544607T T US6678827 B1 US2004181690 A1 WO0069120 A1	21-11-2000 30-01-2002 24-12-2002 13-01-2004 16-09-2004 16-11-2000
US6202157	13-03-2001	US6202157 B1	13-03-2001
US6732168	04-05-2004	US6732168 B1	04-05-2004

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
BORDEN LADNER GERVAIS LLP
World Exchange Plaza
1100 - 100 Queen Street
OTTAWA, Ontario
Canada, K1P 1J9

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 20 June 2005 (20-06-2005)
Applicant's or agent's file reference PAT58913W-90	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/CA2005/000294	International filing date *(day/month/year)* 25 February 2005 (25-02-2005)

Applicant
RESEARCH IN MOTION LIMITED

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19 :
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46) :

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
   1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that :

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for the international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Lucille Leonard (819) 953-1737

(See notes on accompanying sheet)

NOTES TO FROM PCT/ISA/220

These Notes are intended to give instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide,* Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

(Aug 20/05) (Aug 30/05) - entered co checked su

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)) :

The amendments must be submitted with a letter.
The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").
The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged;
(ii) the claim is cancelled;
(iii) the claim is new;
(iv) the claim replaces one or more claims as filed;
(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter :

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
   "Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
   "Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
   "Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
   "Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
   "Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

If a demand for international preliminary examination is made, the written opinion of the International Searching Authority will, except in certain cases where the International Preliminary Examining Authority did not act as International Searching Authority and where it has notified the International Bureau under Rule 66.1*bis*(b), be considered to be a written opinion of the International Preliminary Examining Authority. If a demand is made, the applicant may submit to the International Preliminary Examining Authority a reply to the written opinion together, where appropriate, with amendments before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later (Rule 43*bis*.1(c)).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	System and Method for Configuring Devices for Secure Operations
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	Stephen D. Scanlon/Matthew W. Johnson
Attorney Docket Number:	555255-013133

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	330	330
Utility Search Fee	1111	1	540	540
Utility Examination Fee	1311	1	220	220
Pages:				
Claims:				
Claims in excess of 20	1202	4	52	208
Independent claims in excess of 3	1201	1	220	220
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1518**

Electronic Acknowledgement Receipt

EFS ID:	10520002
Application Number:	13182827
International Application Number:	
Confirmation Number:	7138
Title of Invention:	System and Method for Configuring Devices for Secure Operations
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	89441
Filer:	Stephen D. Scanlon/Matthew W. Johnson
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255-013133
Receipt Date:	14-JUL-2011
Filing Date:	
Time Stamp:	14:53:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1518
RAM confirmation Number	1120
Deposit Account	501432
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		013133_Spec.pdf	1134235 8c83aa025bf9f4225a3fe55a5ae1de7df1ae6620	yes	28

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	20
Claims	21	27
Abstract	28	28

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Drawings-only black and white line drawings	013133_Drawings.pdf	148626 8dc9e01da8d27cbc054a2b5b848b34cd7cdc47b5	no	10
Warnings:					
Information:					
3	Oath or Declaration filed	013133_Decl.pdf	220078 2dcdb6dd55c3c4ccc1130a56c2711fda3fe21a99	no	4
Warnings:					
Information:					
4	Application Data Sheet	013133_ADS.pdf	968711 5b401ea309bd37a8ee3153a8c6d55a541f414e33	no	6
Warnings:					
Information:					
5	Power of Attorney	POA_use.pdf	76172 65a8ae868e733a95b0d6bffa3174c44aea3ef014	no	1
Warnings:					
Information:					
6	Assignee showing of ownership per 37 CFR 3.73(b).	013133_CFR.pdf	59203 a731e3610e2ec10a23db0df1d4355637b507826b	no	1
Warnings:					
Information:					

7	Information Disclosure Statement (IDS) Form (SB08)	IDS_013133.pdf	612760 f5e829a6a984dcf9777d8a1517f76212ca21b91a	no	5
Warnings:					
Information:					
8	Foreign Reference	WO0069120.pdf	3995641 a09bd42e1670cb96163b794c0482884fd498cb3a	no	97
Warnings:					
Information:					
9	Non Patent Literature	Sems.pdf	1298516 e5765b3b3467e47e83bd2a9acc9e8d8d343684bc	no	11
Warnings:					
Information:					
10	Non Patent Literature	Gavrila.pdf	868548 899e2b11c5779c723546948ddb73a59f53c826ad	no	8
Warnings:					
Information:					
11	Non Patent Literature	ISR_June2005.pdf	1061193 22d99e915b530374c2acd2350d38f5ad7a1acb97	no	11
Warnings:					
Information:					
12	Non Patent Literature	EPO_Search_July2007.pdf	115132 2dde1955de8044b1e7c1ffb000d63321e6f7d1e5	no	2
Warnings:					
Information:					
13	Fee Worksheet (SB06)	fee-info.pdf	37636 5ba922a846225a50889d9b554af6f497ab191c89	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	10596451		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. Patent Application No. 11/065,901, filed February 25, 2005, entitled "System and Method for Configuring Devices for Secure Operations," which claims priority to and the benefit of U.S. Provisional Patent Application 60/567,137, filed April 30, 2004, entitled "System and Method for Configuring Devices for Secure Operations," the entirety of both of which is hereby incorporated by reference.

BACKGROUND

Technical Field

The present invention relates generally to the field of communications, and in particular to configuring devices for secure operations.

Description of the Related Art

Mobile wireless communications devices are increasingly being used within corporate and governmental organizations. With the increased usage of mobile devices, companies are faced with the issue of defining and enforcing a secure mode of operation for their deployed devices that they consider secure and in accordance with their corporate or government security policy.

For example, when government agencies purchase and deploy a product that has been validated to FIPS 140-2 ("Security Requirements for Cryptographic Modules") the product is only authorized for use by employees when it operates in a secure mode of operation referred to as the FIPS mode of operation. With the many different security settings that are potentially configurable, the task of defining and configuring a secure mode of operation on an individual IT policy basis for multiple devices is difficult. Also, once a device is configured into a secure mode, the device operator does not have an efficient way to know that the device has been so configured.

BRIEF SUMMARY

In accordance with the teachings disclosed herein, systems and methods are provided for establishing security-related modes of operation for computing devices. As an example of a system and method, a policy data store contains security mode configuration data related to the computing devices. Security mode configuration data is used in establishing a security-related mode of operation for the computing devices.

As another example, a computing device can be configured to utilize a centralized policy data store to implement a security-related mode of operation. The computing device includes a communication interface and a system processor. The communication interface facilitates communication between a centralized policy data store and the computing device. Processing instructions that operate on the computing device include security instructions that place the computing device in a secure mode of operation responsive to configuration data received from the centralized policy data store via the communication interface. The system processor instructions can also include user interface instructions for sending a notification to a display associated with the computing device. The output can include a visual indication of the security mode of operation.

As will be appreciated, the systems and methods disclosed herein are capable of different embodiments, and its details are capable of modifications in various respects. Accordingly, the drawings and description set forth below are to be regarded as illustrative in nature and not restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an overview of an example communication system in which a wireless communication device may be used.

FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices.

FIG. 3 is a block diagram depicting a system wherein an IT (information technology) administrator can collect and store IT security policies.

FIG. 4 is a block diagram depicting different security mode instructions being provided to devices.

FIG. 5 is a block diagram depicting the generation of visual indicators for display to users that indicate the devices' secure mode of operation type.

FIG. 6 is a flowchart depicting an operational scenario wherein a security policy is deployed to multiple devices.

FIG. 7 is a block diagram depicting the deployment of a FIPS mode of operation.

FIGS. 8 and 9 are block diagrams depicting multiple security mode settings being deployed to the devices.

FIG. 10 is a block diagram of an example mobile device.

DETAILED DESCRIPTION OF THE DRAWINGS

FIG. 1 is an overview of an example communication system in which a wireless communication device may be used. One skilled in the art will appreciate that there may be hundreds of different topologies, but the system shown in FIG. 1 helps demonstrate the operation of the encoded message processing systems and methods described in the present application. There may also be many message senders and recipients. The simple system shown in FIG. 1 is for illustrative purposes only, and shows perhaps the most prevalent Internet e-mail environment where security is not generally used.

FIG. 1 shows an e-mail sender 10, the Internet 20, a message server system 40, a wireless gateway 85, wireless infrastructure 90, a wireless network 105 and a mobile communication device 100.

An e-mail sender system 10 may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system 10 has an account, located within a company, possibly connected to a local area network (LAN), and connected to the Internet 20, or connected to the Internet 20 through a large ASP (application service provider) such as America Online (AOL). Those skilled in the art will appreciate that the systems shown in FIG. 1 may instead be connected to a wide area network (WAN) other than the Internet, although e-mail transfers are commonly accomplished through Internet-connected arrangements as shown in FIG. 1.

The message server 40 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 20. Although other messaging systems might not require a message server system 40, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server.

Perhaps the two most common message servers are Microsoft Exchange^{TM} and Lotus Domino^{TM}. These products are often used in conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the secure message processing described below. Message servers such as server 40 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation.

The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 105 to the mobile device 100. The particular network 105 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.

As shown in FIG. 1, a composed e-mail message 15 is sent by the e-mail sender 10, located somewhere on the Internet 20. This message 15 is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 15 arrives at the message server 40 and is normally stored in a message store. Most known messaging systems support a so-called "pull" message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device 100 are redirected from the message server 40 to the mobile device 100 as they are received.

Regardless of the specific mechanism controlling the forwarding of messages to the mobile device 100, the message 15, or possibly a translated or reformatted version thereof, is sent to the wireless gateway 85. The wireless infrastructure 90 includes a series of connections to wireless network 105. These connections could be Integrated Services Digital Network (ISDN), Frame Relay or T1 connections using the TCP/IP protocol used throughout the Internet. As used herein, the term "wireless network" is intended to include three different types of networks, those being (1) data-centric wireless networks, (2) voice-centric wireless networks and (3) dual-mode networks that can support both voice and data communications over the same physical base stations. Combined dual-mode networks include, but are not limited to, (1) Code Division Multiple Access (CDMA) networks, (2) the Groupe Special Mobile or the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) networks, and (3) future third-generation (3G) networks like Enhanced Data-rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS). Some older examples of data-centric network include the Mobitex™ Radio Network and the DataTAC™ Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM, and TDMA systems.

FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices. The system of FIG. 2 is substantially similar to the FIG. 1 system, but includes a host system 30, a redirection program 45, a mobile device cradle 65, a wireless virtual private network (VPN) router 75, an additional wireless network 110 and multiple mobile communication devices 100. As described above in conjunction with FIG. 1, FIG. 2 represents an overview of a sample network topology. Although the encoded message processing systems and methods described herein may be applied to networks having many different topologies, the network of FIG. 2 is useful in understanding an automatic e-mail redirection system mentioned briefly above.

The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100. A more detailed description of the redirection software 45 may be found in the commonly assigned United States Patent 6,219,694 ("the '694 Patent"), entitled "System and Method for Pushing Information From A Host System To A Mobile Data Communication Device Having A Shared Electronic Address", and issued to the assignee of the instant application on April 17, 2001, which is hereby incorporated into the present application by reference. This push technique may use a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device, thus effectively extending the security firewall to include each mobile device 100 associated with the host system 30.

As shown in FIG. 2, there may be many alternative paths for getting information to the mobile device 100. One method for loading information onto the mobile device 100 is through a port designated 50, using a device cradle 65. This method tends to be useful for bulk information updates often performed at initialization of a mobile device 100 with the host system 30 or a computer 35 within the system 30. The other main method for data exchange is over-the-air using wireless networks to deliver the information. As shown in FIG. 2, this may be accomplished through a wireless VPN router 75 or through a traditional Internet connection 95 to a wireless gateway 85 and a wireless infrastructure 90, as described above. The concept of a wireless VPN router 75 is new in the wireless industry and implies that a VPN connection could be established directly through a specific wireless network 110 to a mobile device 100. The possibility of using a wireless VPN router 75 has only recently been available and could be used when the new Internet Protocol (IP) Version 6 (IPV6) arrives into IP-based wireless networks. This new protocol will provide enough IP addresses to dedicate an IP address to every mobile device 100 and thus make it possible to push information to a mobile device 100 at any time. A principal advantage of using this wireless VPN router 75 is that it could be an off-the-shelf VPN component, thus it would not require a separate wireless gateway 85 and wireless infrastructure 90 to be used. A VPN connection would preferably be a Transmission Control Protocol (TCP)/IP or User Datagram Protocol (UDP)/IP connection to deliver the messages directly to the mobile device 100. If a wireless VPN 75 is not available then a link 95 to the Internet 20 is the most common connection mechanism available and has been described above.

In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way, messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the "from" field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.

With reference back to the port 50 and cradle 65 connectivity to the mobile device 100, this connection path offers many advantages for enabling one-time data exchange of large items. For those skilled in the art of personal digital assistants (PDAs) and synchronization, the most common data exchanged over this link is Personal Information Management (PIM) data 55. When exchanged for the first time this data tends to be large in quantity, bulky in nature and requires a large bandwidth to get loaded onto the mobile device 100 where it can be used on the road. This serial link may also be used for other purposes, including setting up a private security key 111 such as an S/MIME or PGP specific private key, the Certificate (Cert) of the user and their Certificate Revocation Lists (CRLs) 60. The private key is preferably exchanged so that the desktop 35 and mobile device 100 share one personality and one method for accessing all mail.

The Cert and CRLs are normally exchanged over such a link because they represent a large amount of the data that is required by the device for S/MIME, PGP and other public key security methods.

FIG. 3 depicts a system wherein an IT (information technology) administrator 200 can collect all applicable IT security policies 202 into one convenient location (e.g., policy data store 210). The placement of IT policies 202 in one location 210 allows an administrator 200 to configure the policies 202 appropriately, and to enable (220) or disable (230) a secure mode defined therein for the devices 250.

Mode instructions (e.g., commands 220 and 230) may be sent to the devices 250 over many different types of data communication links, such as a network 240. Different devices may be connected to the network 240, including mobile devices (e.g., mobile wireless communications device 252) and desktop/laptop computers (e.g., desktop computer 254).

As shown in FIG. 4, the devices 250 can be instructed to be in a first secure mode of operation, and then later they can be switched to a different secure mode of operation. For example, an administrator 200 may send a security mode A enable command 220. Later because of a change in IT security policy, the administrator 200 wishes to raise the security level of the mode in which the devices 250 are operating and therefore sends a security mode B enable command 300 to the devices 250.

FIG. 5 illustrates that the devices 250 can provide some type of an indication to the users of the devices. The indication can be a visual indication 350 which is provided to a user 352. The visual indication 350 indicates to the user 352 that the device 252 is operating in a specific secure mode. For example, it can display in a security options screen that the device 252 is operating in a FIPS mode of operation due to the security configuration sent by the administrator 200.

FIG. 6 depicts an operational scenario wherein a security policy is deployed to multiple devices. At step 400, an IT administrator (or its agent) configures a security policy and deploys it to the devices at step 402. In this operational scenario, an IT administrator can designate and deploy a security mode to multiple devices with minimal effort on the part of the IT administrator. As an illustration, an IT administrator can click an administrator's interface checkbox to designate that all (or most) of the devices should be uniformly operating at security level three.

At step 404, the devices receive the deployed security mode and process the mode command. Processing of the command causes the devices to operate in the defined security mode. At step 406, a user of the device can see an indication of which specific security mode the device has been configured by the IT administrator. At step 408, the IT administrator receives an indication from the devices that the devices have received and entered into the designated secure mode of operation.

It should be understood that similar to the other processing flows described herein, the steps and the order of the steps in the flowchart described herein may be altered, modified and/or augmented and still achieve the desired outcome.

FIG. 7 depicts a system wherein an IT administrator 200 can define a meta IT policy for a FIPS mode of operation 510. The parameters for the FIPS mode of operation 510 are set in accordance with corporate or government security policies 520 (e.g., FIPS 140-2). The defined FIPS mode of operation 510 limits the use of cryptographic algorithms by the devices 250 to those that are FIPS-approved (e.g., AES and Triple DES), and when enabled, forces the devices to use only these algorithms.

FIG. 8 illustrates that multiple security mode settings 630 can be deployed to the devices 250. The policy data store 210 in this example contains a list 600 of devices as well as which security modes should be used for the devices. The policy data store 210 can contain one or more data structures for indicating which devices should utilize which security schemes. For example, a data structure 610 can be used to store which devices should use security mode A settings, and data structure 620 can be used to store which devices should use security mode B settings. FIG. 9 shows that based upon the information contained in the data structures 610 and 620, different settings (e.g., security settings A 700 and security settings B 710) can be deployed to different devices at the same time or at different times.

The systems and methods disclosed herein are presented only by way of example and are not meant to limit the scope of the invention. Other variations of the systems and methods described above will be apparent to those skilled in the art and as such are considered to be within the scope of the invention. For example, the systems and methods disclosed herein may be used with many different computers and devices, such as a wireless mobile communications device shown in FIG. 10. With reference to FIG. 10, the mobile device 100 is a dual-mode mobile device and includes a transceiver 811, a microprocessor 838, a display 822, non-volatile memory 824, random access memory (RAM) 826, one or more auxiliary input/output (I/O) devices 828, a serial port 830, a keyboard 832, a speaker 834, a microphone 836, a short-range wireless communications sub-system 840, and other device sub-systems 842.

The transceiver 811 includes a receiver 812, a transmitter 814, antennas 816 and 818, one or more local oscillators 813, and a digital signal processor (DSP) 820. The antennas 816 and 818 may be antenna elements of a multiple-element antenna, and are preferably embedded antennas. However, the systems and methods described herein are in no way restricted to a particular type of antenna, or even to wireless communication devices.

The mobile device 100 is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device 100 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in FIG. 10 by the communication tower 819. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network.

The transceiver 811 is used to communicate with the network 819, and includes the receiver 812, the transmitter 814, the one or more local oscillators 813 and the DSP 820. The DSP 820 is used to send and receive signals to and from the transceivers 816 and 818, and also provides control information to the receiver 812 and the transmitter 814. If the voice and data communications occur at a single frequency, or closely-spaced sets of frequencies, then a single local oscillator 813 may be used in conjunction with the receiver 812 and the transmitter 814. Alternatively, if different frequencies are utilized for voice communications versus data communications for example, then a plurality of local oscillators 813 can be used to generate a plurality of frequencies corresponding to the voice and data networks 819. Information, which includes both voice and data information, is communicated to and from the transceiver 811 via a link between the DSP 820 and the microprocessor 838.

The detailed design of the transceiver 811, such as frequency band, component selection, power level, etc., will be dependent upon the communication network 819 in which the mobile device 100 is intended to operate. For example, a mobile device 100 intended to operate in a

North American market may include a transceiver 811 designed to operate with any of a variety of voice communication networks, such as the Mobitex or DataTAC mobile data communication networks, AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 100 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with a mobile device 100.

Depending upon the type of network or networks 819, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 819, other than any legally required operations, such as '911' emergency calling.

After any required network registration or activation procedures have been completed, the mobile device 100 may the send and receive communication signals, including both voice and data signals, over the networks 819. Signals received by the antenna 816 from the communication network 819 are routed to the receiver 812, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 820. In a similar manner, signals to be transmitted to the network 819 are processed, including modulation and encoding, for example, by the DSP 820 and are then provided to the transmitter 814 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 819 via the antenna 818.

In addition to processing the communication signals, the DSP 820 also provides for transceiver control. For example, the gain levels applied to communication signals in the receiver 812 and the transmitter 814 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 820. Other transceiver control algorithms could also be implemented in the DSP 820 in order to provide more sophisticated control of the transceiver 811.

The microprocessor 838 preferably manages and controls the overall operation of the mobile device 100. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 820 could be used to carry out the functions of the microprocessor 838. Low-level communication functions, including at least data and voice communications, are performed through the DSP 820 in the transceiver 811. Other, high-level communication applications, such as a voice communication application 824A, and a data communication application 824B may be stored in the non-volatile memory 824 for execution by the microprocessor 838. For example, the voice communication module 824A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 100 and a plurality of other voice or dual-mode devices via the network 819. Similarly, the data communication module 824B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 100 and a plurality of other data devices via the networks 819.

The microprocessor 838 also interacts with other device subsystems, such as the display 822, the RAM 826, the auxiliary input/output (I/O) subsystems 828, the serial port 830, the keyboard 832, the speaker 834, the microphone 836, the short-range communications subsystem 840 and any other device subsystems generally designated as 842.

Some of the subsystems shown in FIG. 10 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as the keyboard 832 and the display 822 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor 838 is preferably stored in a persistent store such as non-volatile memory 824. The non-volatile memory 824 may be implemented, for example, as a Flash memory component, or as battery backed-up RAM. In addition to the operating system, which controls low-level functions of the mobile device 810, the non-volatile memory 824 includes a plurality of software modules 824A-824N that can be executed by the microprocessor 838 (and/or the DSP 820), including a voice communication module 824A, a data communication module 824B, and a plurality of other operational modules 824N for carrying out a plurality of other functions. These modules are executed by the microprocessor 838 and provide a high-level interface between a user and the mobile device 100. This interface typically includes a graphical component provided through the display 822, and an input/output component provided through the auxiliary I/O 828, keyboard 832, speaker 834, and microphone 836. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 826 for faster operation.

Moreover, received communication signals may also be temporarily stored to RAM 826, before permanently writing them to a file system located in a persistent store such as the Flash memory 824.

An exemplary application module 824N that may be loaded onto the mobile device 100 is a personal information manager (PIM) application providing PDA functionality, such as calendar events, appointments, and task items. This module 824N may also interact with the voice communication module 824A for managing phone calls, voice mails, etc., and may also interact with the data communication module for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 824A and the data communication module 824B may be integrated into the PIM module.

The non-volatile memory 824 preferably also provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 824A, 824B, via the wireless networks 819. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless networks 819, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

Context objects representing at least partially decoded data items, as well as fully decoded data items, are preferably stored on the mobile device 100 in a volatile and non-persistent store such as the RAM 826. Such information may instead be stored in the non-volatile memory 824, for example, when storage intervals are relatively short, such that the information is removed from memory soon after it is stored. However, storage of this information in the RAM 826 or another volatile and non-persistent store is preferred, in order to ensure that the information is erased from memory when the mobile device 100 loses power. This prevents an unauthorized party from obtaining any stored decoded or partially decoded information by removing a memory chip from the mobile device 100, for example.

The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 830 of the mobile device 100 to the serial port of a computer system or device. The serial port 830 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 824N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 819. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 830. For example, a USB port would provide an interface to a similarly equipped personal computer.

Additional application modules 824N may be loaded onto the mobile device 100 through the networks 819, through an auxiliary I/O subsystem 828, through the serial port 830, through the short-range communications subsystem 840, or through any other suitable subsystem 842, and installed by a user in the non-volatile memory 824 or RAM 826. Such flexibility in application installation increases the functionality of the mobile device 100 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 100.

When the mobile device 100 is operating in a data communication mode, a received signal, such as a text message or a web page download, is processed by the transceiver module 811 and provided to the microprocessor 838, which preferably further processes the received signal in multiple stages as described above, for eventual output to the display 822, or, alternatively, to an auxiliary I/O device 828. A user of mobile device 100 may also compose data items, such as e-mail messages, using the keyboard 832, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 100 is further enhanced with a plurality of auxiliary I/O devices 828, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the communication networks 819 via the transceiver module 811.

When the mobile device 100 is operating in a voice communication mode, the overall operation of the mobile device is substantially similar to the data mode, except that received signals are preferably be output to the speaker 834 and voice signals for transmission are generated by a microphone 836. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile device 100. Although voice or audio signal output is preferably accomplished primarily through the speaker 834, the display 822 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 838, in conjunction with the voice communication module and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 822.

A short-range communications subsystem 840 is also included in the mobile device 100. The subsystem 840 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a Bluetooth^{TM} module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that “Bluetooth” and “802.11” refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.

The systems’ and methods’ data may be stored in one or more data stores. The data stores can be of many different types of storage devices and programming constructs, such as RAM, ROM, Flash memory, programming data structures, programming variables, etc. It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program.

The systems and methods may be provided on many different types of computer-readable media including computer storage mechanisms (e.g., CD-ROM, diskette, RAM, flash memory, computer’s hard drive, etc.) that contain instructions for use in execution by a processor to perform the methods’ operations and implement the systems described herein.

The computer components, software modules, functions and data structures described herein may be connected directly or indirectly to each other in order to allow the flow of data needed for their operations. It is also noted that a module or processor includes but is not limited to a unit of code that performs a software operation, and can be implemented for example as a subroutine unit of code, or as a software function unit of code, or as an object (as in an object-oriented paradigm), or as an applet, or in a computer script language, or as another type of computer code.

WHAT IS CLAIMED IS:

1. A system for use in establishing a security-related mode of operation for computing devices, comprising:

a policy data store for storing configuration data related to a plurality of computing devices;

a security mode data structure contained within the policy data store;

wherein the security mode data structure stores a security mode of operation;

wherein the stored security mode of operation is provided to the plurality of computing devices over a network;

wherein the security mode of operation places the plurality of computing devices in a predetermined security mode of operation;

wherein at least one of the plurality of computing devices comprises user interface instructions configured to send an output to a display associated with the one of the plurality of computing devices, the output being configured to comprise a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, wherein the security mode of operation forces use of one or more cryptographic algorithms.

2. The system of claim 1, wherein the security mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation.

3. The system of claim 2, wherein the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

4. The system of claim 1, wherein the security mode data structure comprises a first security mode data structure and a second security mode data structure;

wherein the first security mode data structure includes a first security mode being associated with a first plurality of computing devices;

wherein the second security mode data structure includes a second security mode being associated with a second plurality of computing devices.

5. The system of claim 4, wherein the first security mode of operation contained in the first data structure is communicated to the first plurality of computing devices in order to place the first plurality of computing devices in the first security mode;

wherein the second security mode of operation contained in the second data structure is communicated to the second plurality of computing devices in order to place the second plurality of computing devices in the second security mode.

6. The system of claim 5, wherein the providing of the first security mode data structure to the first plurality of devices causes the devices in the first plurality of devices to be placed in a FIPS mode of operation that includes required use of AES encryption;

wherein the providing of the second security mode data structure to the second plurality of devices causes the devices in the second plurality of devices to be placed in a FIPS mode of operation that includes required use of Triple DES (3DES) encryption.

7. The system of claim 1, wherein at least one of the plurality of computing devices receives a disable message for disabling the security mode of operation of the one of the plurality of computing devices.

8. The system of claim 1, wherein the policy data store stores IT security policies related to the plurality of computing devices;

wherein an administrator defines through the interface a meta IT policy for a security mode of operation;

wherein the defined security mode of operation limits the use of cryptographic algorithms by the devices to those that are specified by the meta IT policy.

9. The system of claim 8, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

10. A computing device utilizing a centralized policy data store to implement a security-related mode of operation, the device comprising:

a communication interface configured to facilitate communication between the centralized policy data store and the computing device; and

a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions;

wherein the processing instructions includes security instructions configured to place the computing device in a security mode of operation responsive to configuration data received from the centralized policy data store via the communication interface;

wherein the computing device comprises user interface instructions configured to send an output to a display associated with the computing device, the output being configured to comprise a visual indication of the security mode of operation to the device's user, wherein the security mode of operation forces use of one or more cryptographic algorithms.

11. The device of claim 10, wherein the processing instructions further comprise user interface instructions configured to send an output to a display associated with the computing device, the output having a visual indication of the security mode of operation that is visible to the device's user.

12. The device of claim 11, wherein the visual indication of the security mode is provided by a security options screen.

13. The device of claim 12, wherein the security instructions are configured to update the security mode of operation responsive to a change in the configuration data stored on the centralized policy data store, wherein a visual indication is provided to the device's user to indicate the updated security mode of operation.

14. The device of claim 13, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

15. The device of claim 10, wherein the configuration data stored on the centralized policy data store comprises a plurality of security mode data structures contained within the policy data store.

16. The device of claim 15, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

17. A method for use in establishing a security-related mode of operation for a computing device, comprising:

storing a security mode of operation in a policy data store;

sending the stored security mode of operation to the computing device over a network;

wherein the sent security mode of operation places the computing device into a predetermined security-related mode of operation;

wherein the computing device comprises user interface instructions configured to send an output to a display associated with the computing device, the output being configured to comprise a visual indication of the security mode of operation to the device's user, wherein the security mode of operation forces use of one or more cryptographic algorithms.

18. The method of claim 17, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

19. The method of claim 17, further comprising the step of displaying the security mode of operation of the computing device by providing a visual indication on a screen of the computing device.

20. The method of claim 17, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

21. The method of claim 17, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

22. A digital signal containing the sent security mode of operation of claim 17.

23. Computer software stored on one or more non-transitory computer readable media, the computer software comprising program code for carrying out a method according to claim 17.

24. A system for establishing a security-related mode of operation for a computing device, comprising:

means for receiving a security mode of operation from a server, the server comprising a security mode data structure comprising security mode data for a plurality of computing devices;

means for entering the security mode of operation received from the server, wherein the means for entering includes means for forcing use of AES or 3DES;

means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device, wherein the security mode of operation forces use of one or more cryptographic algorithms.

ABSTRACT

Systems and methods for establishing a security-related mode of operation for computing devices. A policy data store contains security mode configuration data related to the computing devices. Security mode configuration data is used in establishing a security-related mode of operation for the computing devices.

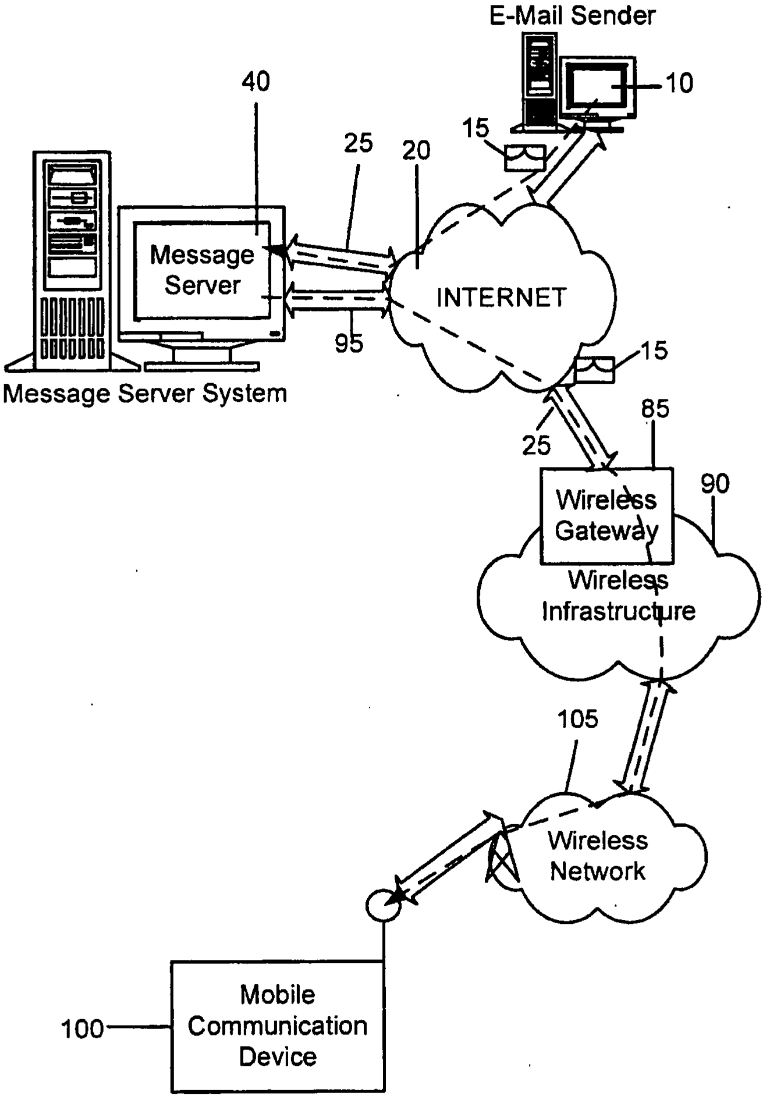

E-Mail Sender
10
15
40
25
20
Message Server
INTERNET
95
Message Server System
15
85
25
90
Wireless Gateway
Wireless Infrastructure
105
Wireless Network
100
Mobile Communication Device

FIG. 1

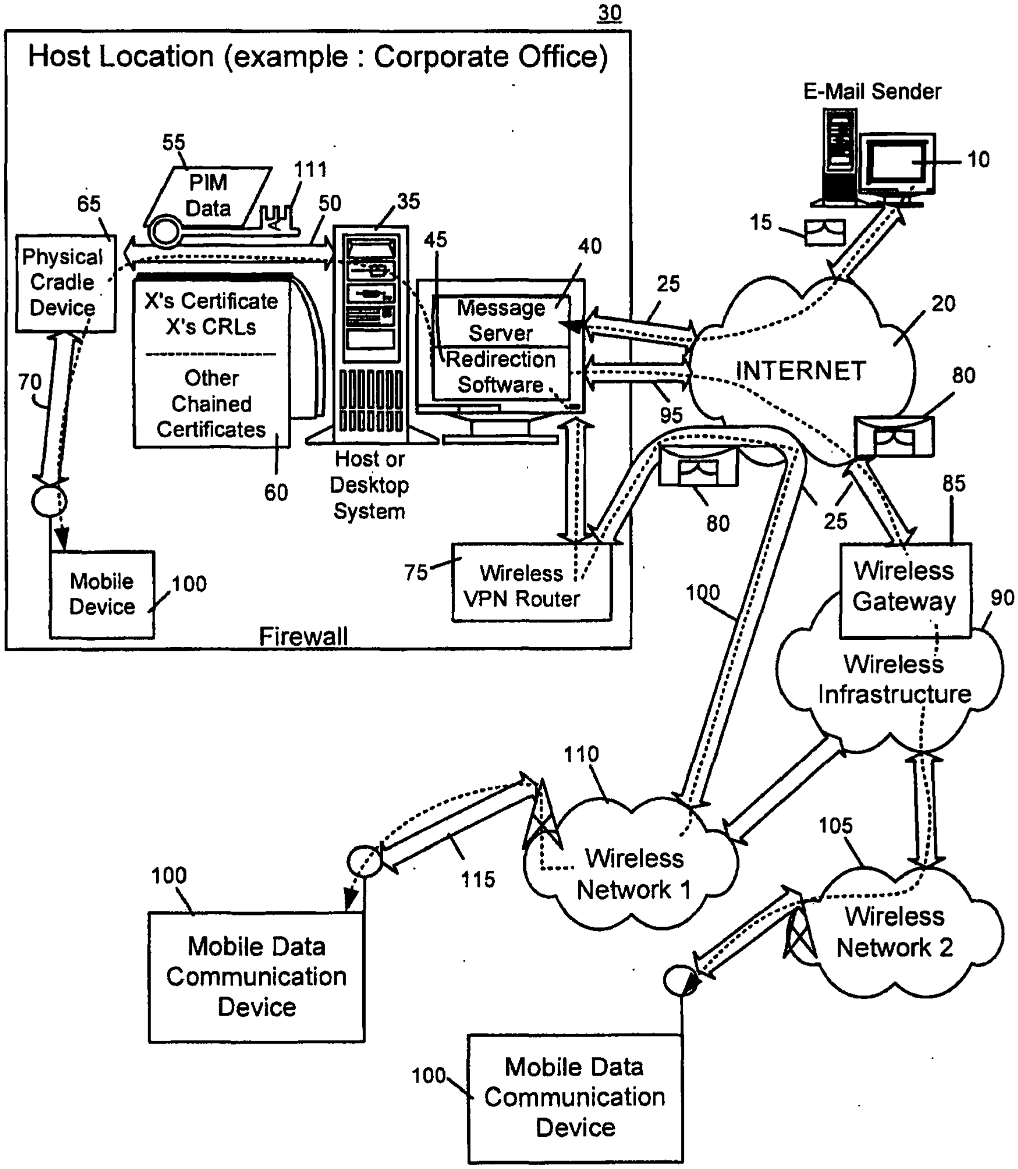

30
Host Location (example : Corporate Office)
E-Mail Sender
10
15
55
PIM Data
111
65
50
35
45
40
Physical Cradle Device
X's Certificate
X's CRLs
Other Chained Certificates
Message Server
Redirection Software
25
INTERNET
20
80
95
70
60
Host or Desktop System
80
25
85
Mobile Device
100
75
Wireless VPN Router
100
Wireless Gateway
90
Firewall
Wireless Infrastructure
110
105
Wireless Network 1
115
100
Wireless Network 2
Mobile Data Communication Device
100
Mobile Data Communication Device

FIG. 2

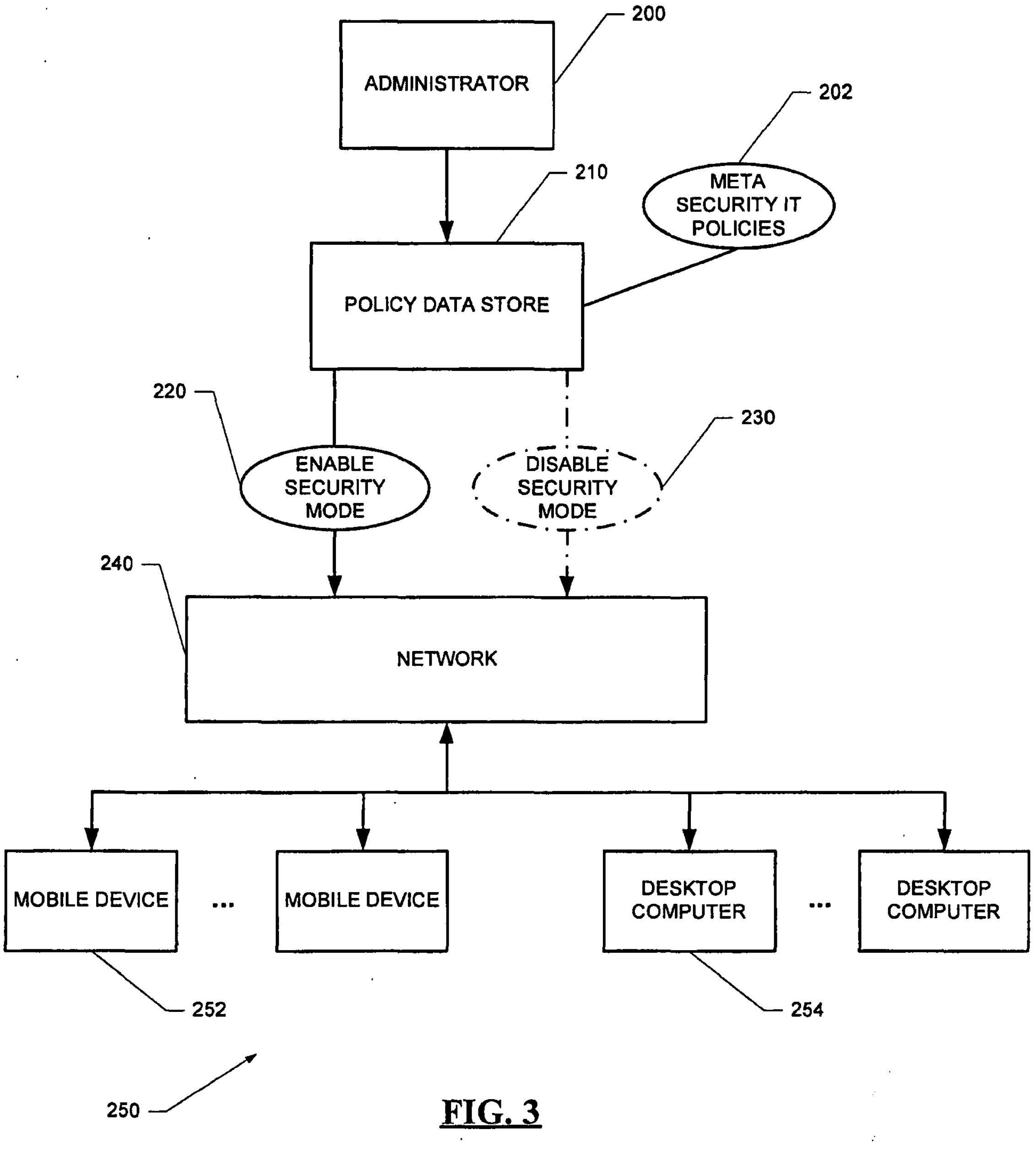

200
ADMINISTRATOR
202
META SECURITY IT POLICIES
210
POLICY DATA STORE
220
ENABLE SECURITY MODE
230
DISABLE SECURITY MODE
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
254
250

FIG. 3

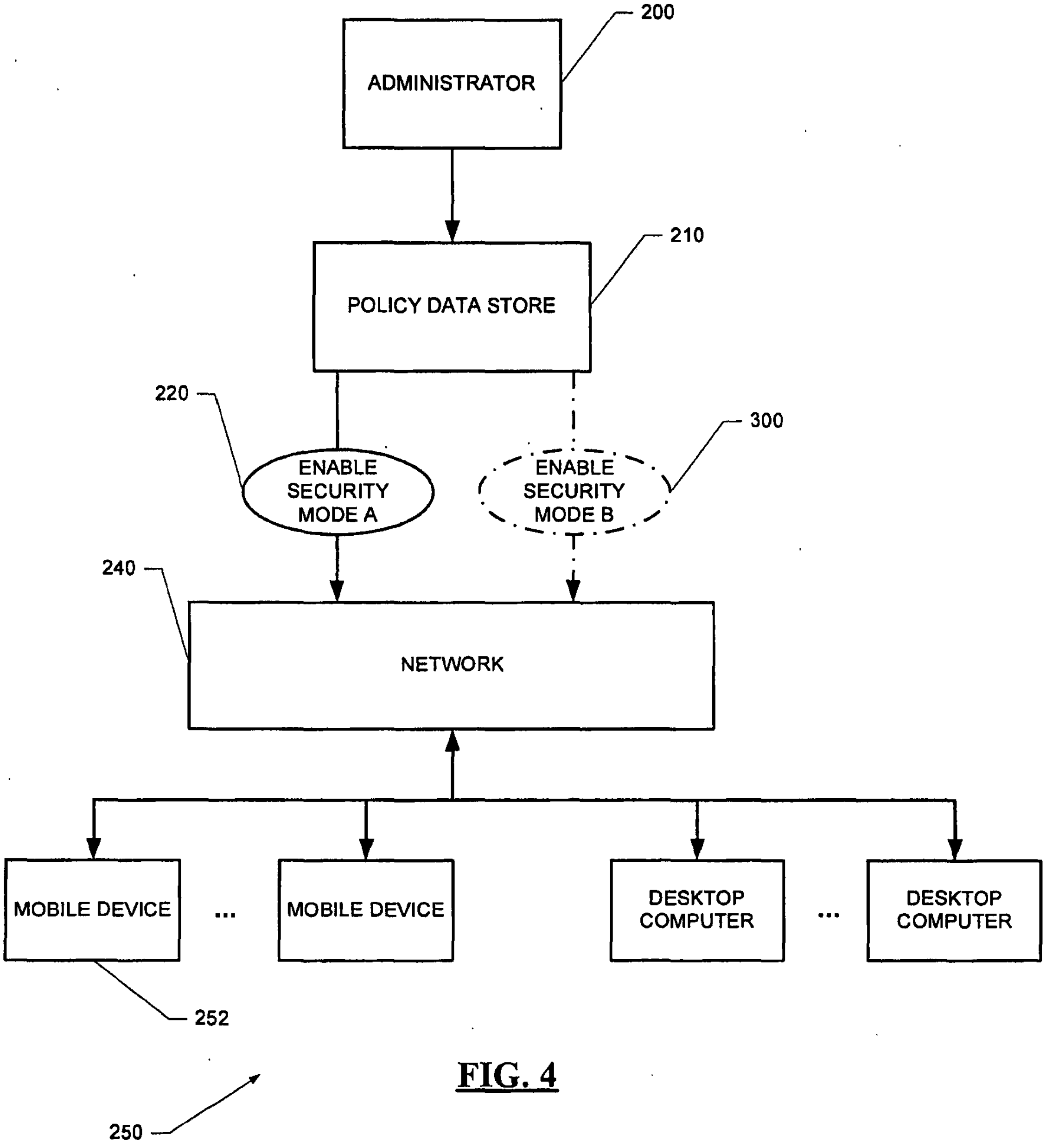

200
ADMINISTRATOR
210
POLICY DATA STORE
220
300
ENABLE SECURITY MODE A
ENABLE SECURITY MODE B
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
250

FIG. 4

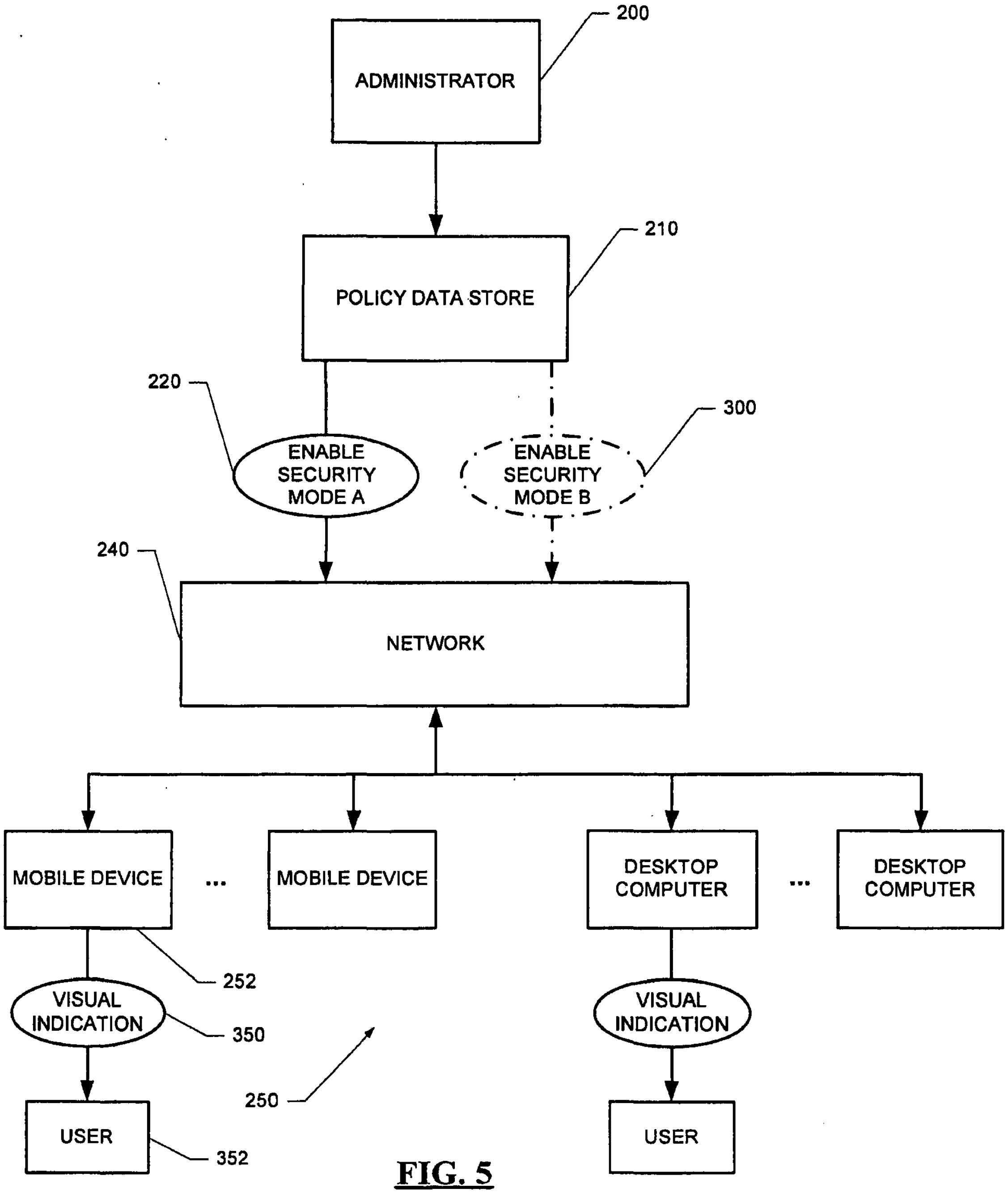

200
ADMINISTRATOR
210
POLICY DATA STORE
220
ENABLE SECURITY MODE A
300
ENABLE SECURITY MODE B
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
VISUAL INDICATION
350
VISUAL INDICATION
250
USER
352
USER

FIG. 5

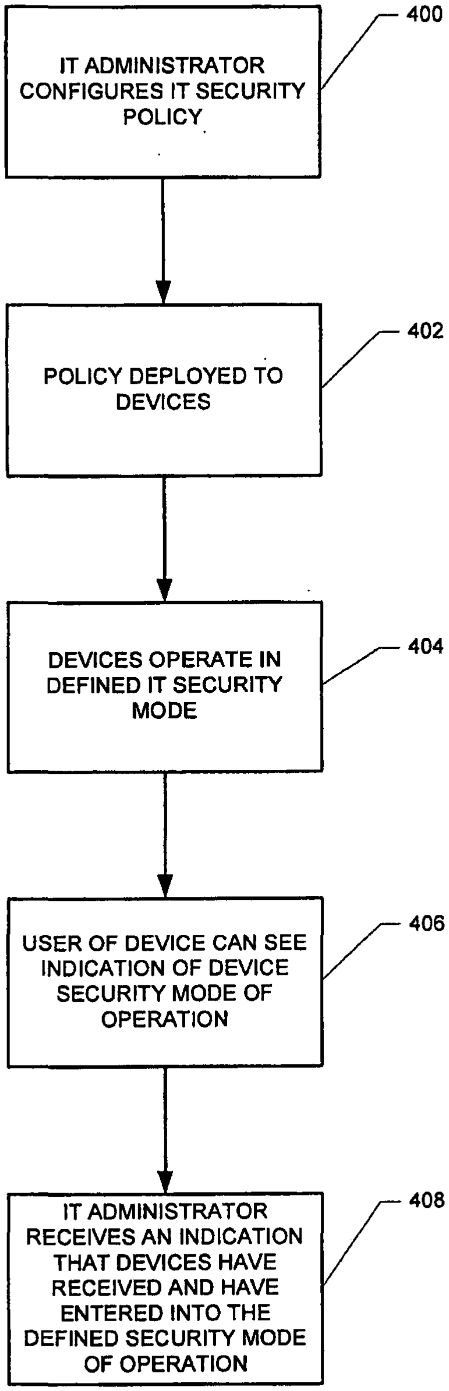

IT ADMINISTRATOR CONFIGURES IT SECURITY POLICY
400
POLICY DEPLOYED TO DEVICES
402
DEVICES OPERATE IN DEFINED IT SECURITY MODE
404
USER OF DEVICE CAN SEE INDICATION OF DEVICE SECURITY MODE OF OPERATION
406
IT ADMINISTRATOR RECEIVES AN INDICATION THAT DEVICES HAVE RECEIVED AND HAVE ENTERED INTO THE DEFINED SECURITY MODE OF OPERATION
408

FIG. 6

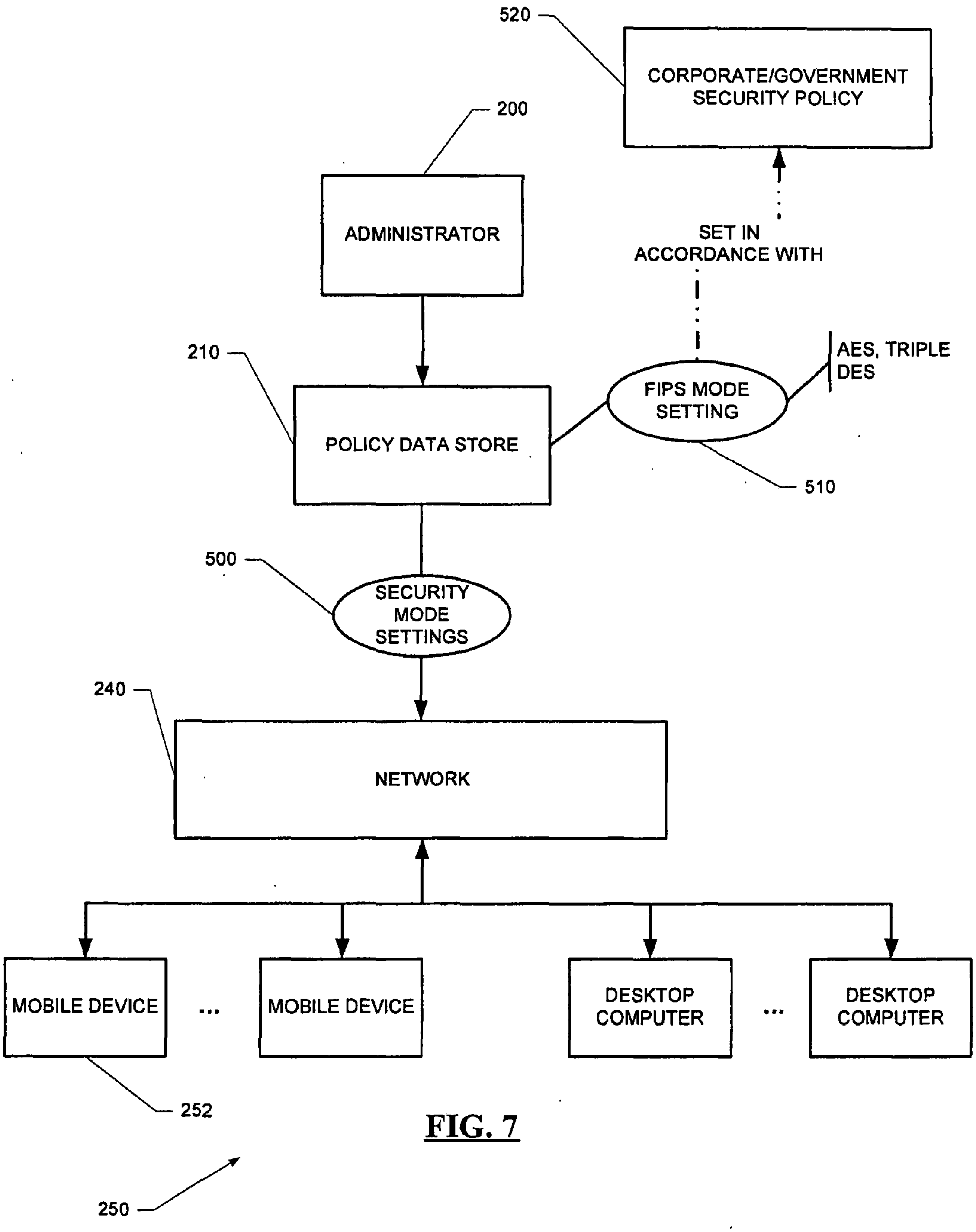

520
CORPORATE/GOVERNMENT SECURITY POLICY
200
ADMINISTRATOR
SET IN ACCORDANCE WITH
210
POLICY DATA STORE
FIPS MODE SETTING
AES, TRIPLE DES
510
500
SECURITY MODE SETTINGS
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
250

FIG. 7

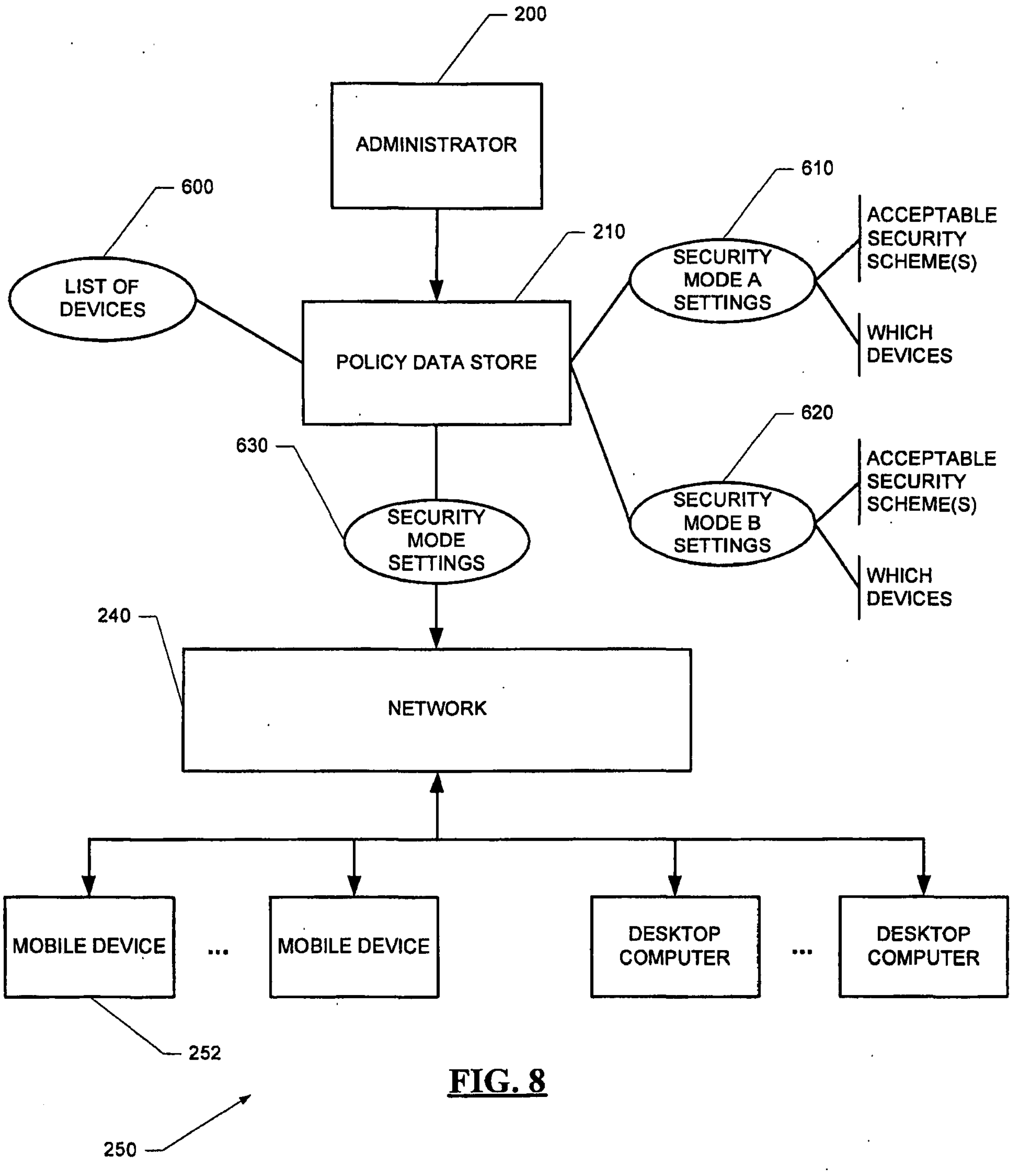

200
ADMINISTRATOR
600
LIST OF DEVICES
210
POLICY DATA STORE
610
SECURITY MODE A SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
620
SECURITY MODE B SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
630
SECURITY MODE SETTINGS
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
250

FIG. 8

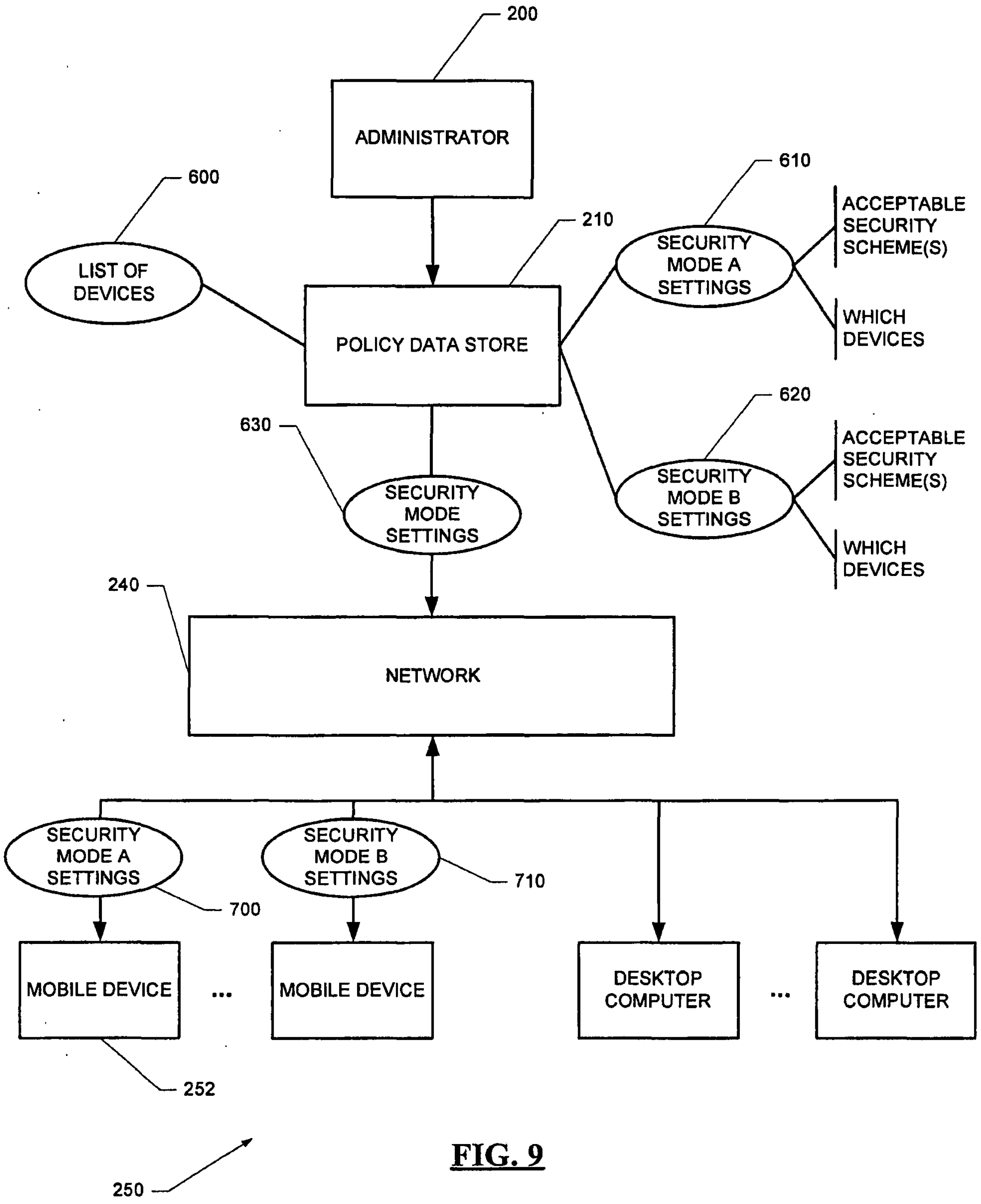

200
ADMINISTRATOR
600
LIST OF DEVICES
210
POLICY DATA STORE
610
SECURITY MODE A SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
620
SECURITY MODE B SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
630
SECURITY MODE SETTINGS
240
NETWORK
SECURITY MODE A SETTINGS
700
SECURITY MODE B SETTINGS
710
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
250

FIG. 9

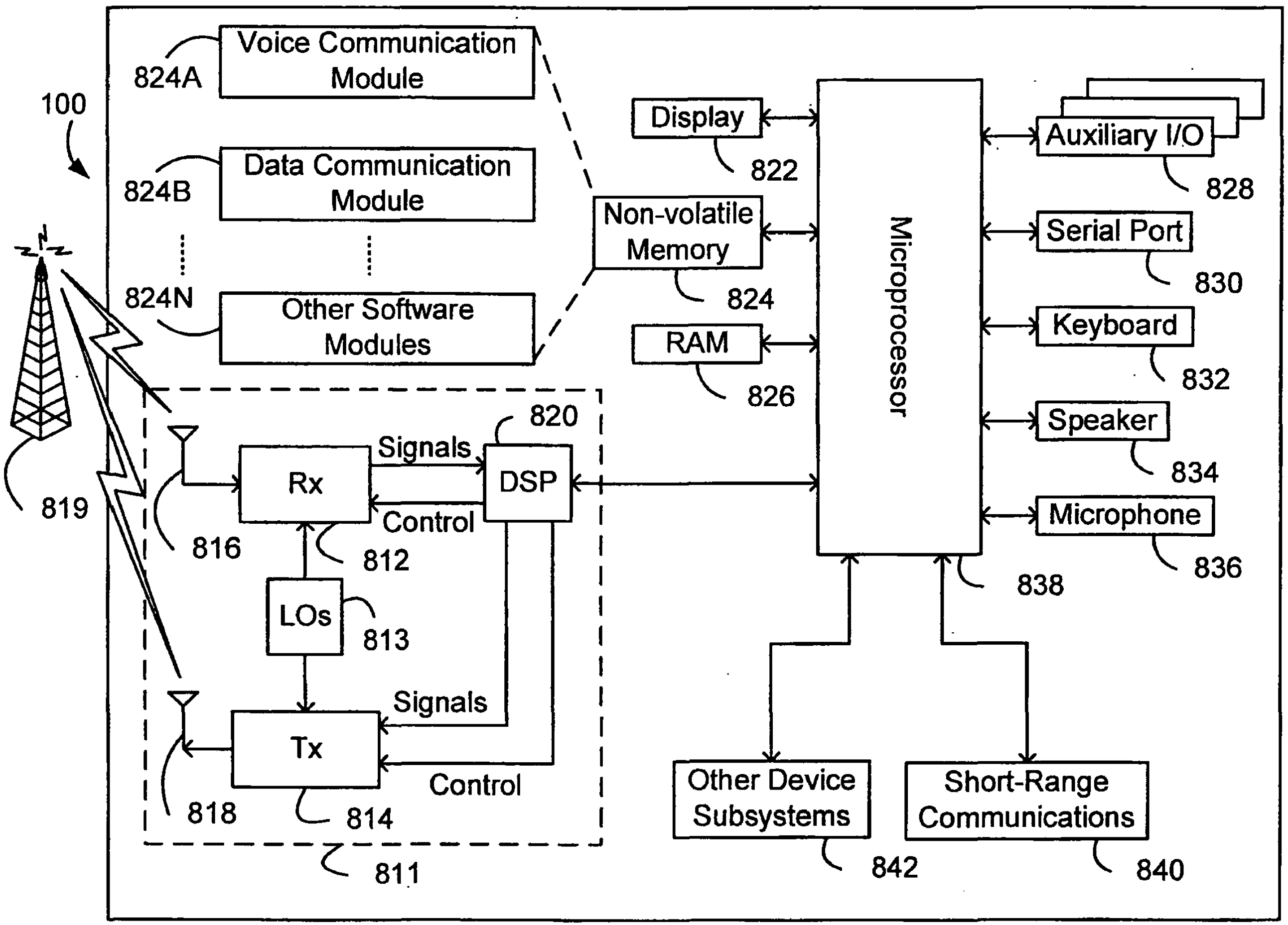

100
Voice Communication Module
824A
Data Communication Module
824B
Other Software Modules
824N
Display
822
Non-volatile Memory
824
RAM
826
Microprocessor
Auxiliary I/O
828
Serial Port
830
Keyboard
832
Speaker
834
Microphone
836
838
819
820
Signals
Rx
DSP
Control
816
812
LOs
813
Signals
Tx
Control
818
814
811
Other Device Subsystems
842
Short-Range Communications
840

FIG. 10

PTO/SB/01 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

□ Declaration Submitted With Initial Filing OR ☑ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	555255012798
First Named Inventor	Neil P. Adams
COMPLETE IF KNOWN	
Application Number	11/065,901
Filing Date	February 25, 2005
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned

I hereby declare that:

Each inventor's residence, mailing address, and citizenship are as stated below next to their name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

(Title of the Invention)

the specification of which

□ is attached hereto

OR

☑ was filed on (MM/DD/YYYY) 02/25/2005 as United States Application Number or PCT International Application Number 11/065,901 and was amended on (MM/DD/YYYY) ______ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? Yes	No
			□	□	□
			□	□	□
			□	□	□
			□	□	□

□ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/01 (06-03)
Approved for use through 07/31/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: □ Customer Number: OR ☑ Correspondence address below

Name
John V. Biernacki, Esq.

Address
JONES DAY - North Point, 901 Lakeside Avenue

City Cleveland	State Ohio	ZIP 44114

Country U.S.A.	Telephone 216-586-3939	Fax 216-579-0212

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]) Neil P.	Family Name or Surname Adams
Inventor's Signature Neil Adams	Date JUL 2 2 2005

Residence: City Waterloo	State Ontario	Country Canada	Citizenship Canadian

Mailing Address
295 Phillip Street

City Waterloo	State Ontario	ZIP N2L 3W8	Country Canada

NAME OF SECOND INVENTOR: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]) Michael K.	Family Name or Surname Brown
Inventor's Signature	Date JUL 2 2 2005

Residence: City Peterborough	State Ontario	Country Canada	Citizenship Canadian

Mailing Address
295 Phillip Street

City Waterloo	State Ontario	ZIP N2L 3W8	Country Canada

☑ Additional inventors or a legal representative are being named on the 2 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto.

[Page 2 of 2]

PTO/SB/02A (08-03)
Approved for use through 08/31/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet Page 1 of 2

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any)): Michael S.
Family Name or Surname: Brown

Inventor's Signature
Date JUL 2 2 2005

Residence: City Waterloo State Ontario Country Canada Citizenship Canadian

Mailing Address 295 Phillip Street

Mailing Address

City Waterloo State Ontario Zip N2L 3W8 Country Canada

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any)): Michael G.
Family Name or Surname: Kirkup

Inventor's Signature Michael Kirkup
Date JUL 2 5 2005

Residence: City Waterloo State Ontario Country Canada Canadian Citizenship

Mailing Address 295 Phillip Street

Mailing Address

City Waterloo State Ontario Zip N2L 3W8 Country Canada

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any)): Herbert A.
Family Name or Surname: Little

Inventor's Signature Herb a Little
Date JUL 2 2 2005

Residence: City Waterloo State Ontario Country Canada Canadian Citizenship

Mailing Address 295 Phillip Street

Mailing Address

City Waterloo State Ontario Zip N2L 3W8 Country Canada

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/02A (08-03)
Approved for use through 08/31/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION	**ADDITIONAL INVENTOR(S)** Supplemental Sheet Page 2 of 2

Name of Additional Joint Inventor, if any:	□ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
David Victor	MacFarlane		
Inventor's Signature		Date JUL 2 2 2005	
Residence: City Waterloo	State Ontario	Country Canada	Citizenship Canadian
Mailing Address 295 Phillip Street			
Mailing Address			
City Waterloo	State Ontario	Zip N2L 3W8	Country Canada
Name of Additional Joint Inventor, if any:	□ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Ian M.	Robertson		
Inventor's Signature	Date JUL 2 2 2005		
Residence: City Waterloo	State Ontario	Country Canada	Canadian Citizenship
Mailing Address 295 Phillip Street			
Mailing Address			
City Waterloo	State Ontario	Zip N2L 3W8	Country Canada
Name of Additional Joint Inventor, if any:	□ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Inventor's Signature	Date		
Residence: City	State	Country	Citizenship
Mailing Address			
Mailing Address			
City	State	Zip	Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	555255-013133
	Application Number	

Title of Invention	System and Method for Configuring Devices for Secure Operations

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

□ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority	● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Neil	P.	Adams	

Residence Information (Select One) ○ US Residency ● Non US Residency ○ Active US Military Service

City	Waterloo	**Country Of Residence** i	CA
Citizenship under 37 CFR 1.41(b) i	CA		

Mailing Address of Applicant:

Address 1	295 Phillip Street		
Address 2			
City	Waterloo	**State/Province**	ON
Postal Code	N2L 3W8	**Country** i	CA

Applicant 2 Remove

Applicant Authority	● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Michael	K.	Brown	

Residence Information (Select One) ○ US Residency ● Non US Residency ○ Active US Military Service

City	Waterloo	**Country Of Residence** i	CA
Citizenship under 37 CFR 1.41(b) i	CA		

Mailing Address of Applicant:

Address 1	295 Phillip Street		
Address 2			
City	Waterloo	**State/Province**	ON
Postal Code	N2L 3W8	**Country** i	CA

Applicant 3 Remove

Applicant Authority	● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Michael	S.	Brown	

Residence Information (Select One) ○ US Residency ● Non US Residency ○ Active US Military Service

City	Waterloo	**Country Of Residence** i	CA

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	555255-013133
	Application Number	

Title of Invention	System and Method for Configuring Devices for Secure Operations

Citizenship under 37 CFR 1.41(b) i	CA		
Mailing Address of Applicant:			
Address 1	295 Phillip Street		
Address 2			
City	Waterloo	**State/Province**	ON
Postal Code	N2L 3W8	**Country**i	CA

Applicant 4 Remove

Applicant Authority	● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118	
Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Michael	G.	Kirkup	
Residence Information (Select One)	○ US Residency	● Non US Residency	○ Active US Military Service	
City	Waterloo	**Country Of Residence** i	CA	
Citizenship under 37 CFR 1.41(b) i	CA			
Mailing Address of Applicant:				
Address 1	295 Phillip Street			
Address 2				
City	Waterloo	**State/Province**	ON	
Postal Code	N2L 3W8	**Country**i	CA	

Applicant 5 Remove

Applicant Authority	● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118	
Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Herbert	A.	Little	
Residence Information (Select One)	○ US Residency	● Non US Residency	○ Active US Military Service	
City	Waterloo	**Country Of Residence** i	CA	
Citizenship under 37 CFR 1.41(b) i	CA			
Mailing Address of Applicant:				
Address 1	295 Phillip Street			
Address 2				
City	Waterloo	**State/Province**	ON	
Postal Code	N2L 3W8	**Country**i	CA	

Applicant 6 Remove

Applicant Authority	● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118	
Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	David	Victor	MacFarlane	
Residence Information (Select One)	○ US Residency	● Non US Residency	○ Active US Military Service	
City	Waterloo	**Country Of Residence** i	CA	
Citizenship under 37 CFR 1.41(b) i	CA			

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	555255-013133
	Application Number	
Title of Invention	System and Method for Configuring Devices for Secure Operations	

Mailing Address of Applicant:			
Address 1	295 Phillip Street		
Address 2			
City	Waterloo	**State/Province**	ON
Postal Code	N2L 3W8	**Country**i	CA

Applicant 7 Remove

Applicant Authority ● Inventor	○ Legal Representative under 35 U.S.C. 117	○ Party of Interest under 35 U.S.C. 118		
Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Ian	M.	Robertson	

Residence Information (Select One) ○ US Residency ● Non US Residency ○ Active US Military Service

City	Waterloo	**Country Of Residence**i	CA
Citizenship under 37 CFR 1.41(b) i	CA		
Mailing Address of Applicant:			
Address 1	295 Phillip Street		
Address 2			
City	Waterloo	**State/Province**	ON
Postal Code	N2L 3W8	**Country**i	CA

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

□ **An Address is being provided for the correspondence Information of this application.**

Customer Number	89441	
Email Address		Add Email Remove Email

Application Information:

Title of the Invention	System and Method for Configuring Devices for Secure Operations		
Attorney Docket Number	555255-013133	**Small Entity Status Claimed** □	
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	10	**Suggested Figure for Publication (if any)**	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	555255-013133
	Application Number	
Title of Invention	System and Method for Configuring Devices for Secure Operations	

Publication Information:

□	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
□	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89441		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	11065901	2005-02-25
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11065901	non provisional of	60567137	2004-04-30

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

			Remove
Application Number	Country i	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ● No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	555255-013133
	Application Number	
Title of Invention	System and Method for Configuring Devices for Secure Operations	

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

If the Assignee is an Organization check here. ☒

Organization Name	Research In Motion Limited		
Mailing Address Information:			
Address 1	295 Phillip Street		
Address 2			
City	Waterloo	**State/Province**	ON
Country i	CA	Postal Code	N2L 3W8
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Matthew W. Johnson/			Date (YYYY-MM-DD)	2011-07-14
First Name	Matthew W.	Last Name	Johnson	Registration Number	59108

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/182,827	07/14/2011	2431	1518	555255-013133	24	4

CONFIRMATION NO. 7138

FILING RECEIPT

OC000000048955186

89441
Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Date Mailed: 07/29/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Neil P. Adams, Waterloo, CANADA;
Michael K. Brown, Waterloo, CANADA;
Michael S. Brown, Waterloo, CANADA;
Michael G. Kirkup, Waterloo, CANADA;
Herbert A. Little, Waterloo, CANADA;
David Victor MacFarlane, Waterloo, CANADA;
Ian M. Robertson, Waterloo, CANADA;

Assignment For Published Patent Application

RESEARCH IN MOTION LIMITED, Waterloo, CANADA

Power of Attorney: The patent practitioners associated with Customer Number 89441

Domestic Priority data as claimed by applicant

This application is a CON of 11/065,901 02/25/2005
which claims benefit of 60/567,137 04/30/2004

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 07/25/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/182,827**

Projected Publication Date: 11/03/2011

Non-Publication Request: No

Early Publication Request: No

Title

System and Method for Configuring Devices for Secure Operations

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

MOBILEIRON, INC. - EXHIBIT 1003
Page 171

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/182,827	07/14/2011	Neil P. Adams	555255-013133

CONFIRMATION NO. 7138

POA ACCEPTANCE LETTER

OC000000048955113

89441
Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Date Mailed: 07/29/2011

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/14/2011.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ltaba/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
13/182,827

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	540
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220
TOTAL CLAIMS (37 CFR 1.16(i))	24 minus 20=	* 4			OR	x 52 =	208
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1				x 220 =	220
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
			TOTAL			TOTAL	1518

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/182,827	07/14/2011	Neil P. Adams	555255-013133

CONFIRMATION NO. 7138

PUBLICATION NOTICE

OC000000050783722

89441
Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Title: System and Method for Configuring Devices for Secure Operations

Publication No.US-2011-0271322-A1
Publication Date:11/03/2011

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/182,827	07/14/2011	Neil P. Adams	555255-013133	7138

89441 7590 08/08/2012

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
08/08/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

dlpejeau@jonesday.com
portfolioprosecution@rim.com

Office Action Summary	**Application No.** 13/182,827	**Applicant(s)** ADAMS ET AL.	
	Examiner BRYAN WRIGHT	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-24* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-24* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *7/24/2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *7/14/2011*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAIL ACTION

1. This action is in response to original fillings on filed 7/14/2011. Claims 1-24 are pending.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 10, 17 and 24 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 8,010,989. Although the conflicting claims are not identical, they are not patentably distinct from each other because both sets of claims are drawn to placing a device into a cryptographic mode and indicating the mode to the user.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 22 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 22 is directed to a “signal”. The Examiner contends in accordance with the MPEP, a “signal" is considered non-statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 4-20, and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen et al. (US Patent Publication No. 2003/0204722 and Schoen hereinafter) in view of Phillps et al. (US Patent Publication No. 2005/0183138 and Phillips hereinafter) and further in view of Scheidt et al. (US Patent No. 6,490,680 and Scheidt hereinafter).

3. As to claims 1, 10, 17 and 24, Schoen discloses a system for use in establishing a security- related mode of operation for computing devices, comprising:

a policy data store for storing configuration data related to a plurality of computing devices (par. 9, lines 12- 15);

a security mode data structure contained within the policy data store (abstract: lines 12-14; par. 33);

where the stored security mode of operation is provided to the computing devices over a network (par. 73, lines 16-20);

where at least one of the plurality of computing devices comprise user interface instructions configured to send an output to a display associated with the one of the plurality of computing device (par. 65, lines 17- 21).

Schoen does not expressly teach the claim limitation element of the output being configured to comprise a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schoen as introduced by Phillips. Phillips discloses the claim limitation element of the output being configured to comprise a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, wherein the security mode of operation forces use of one or more cryptographic algorithm (to provide a visual indication for display to a device user that is indicative of the determined security- related level [par. 96]). Therefore, given the teachings of Phillips, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schoen by employing the well known feature of visually indicating a security level disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

The system of Schoen and Phillips do not expressly teach:

where the security mode data structure stores a security mode of operation,

wherein the security mode of operation forces use of one or more security algorithms.

where the security mode of operation places the computing devices in a predetermined security mode of operation. However in this instance the Examiner notes the teachings of Scheidt. Scheidt is noted to teach in column 8, different security modes and placing the device to a particular security mode. The security modes based on a particular encryption algorithm. Therefore, given the system described above by Schoen and Phillips, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the system enhance data security by employing Scheidt's cryptographic security modes.

4. As to claim 4, Schoen discloses a system where the security mode data structure comprises a first security mode data structure and a second security mode data structure; where the first security mode data structure includes a first security mode being associated with a first plurality of computing devices (par. 73, lines 16-23); where the second security mode data structure includes a second security mode being associated with a second plurality of computing devices (par. 73, lines 16-23).

5. As to claim 5, Schoen discloses a system where the first security mode of operation contained in the first data structure is communicated to the first plurality of computing devices in order to place the first plurality of computing devices in the first security mode (par. 73, lines 16-23); where the second security mode of operation contained in the second data structure is communicated to the second plurality of computing devices in order to place the second plurality of computing devices in the second security mode (par. 73, lines 16-23).

6. As to claim 6, Schoen discloses a system where an administrator uses an interface to update the configuration data related to a plurality of computing devices that is stored in the policy data store, and uses an interface to communicate security modes

of operation to the computing devices (par. 69, lines 21-32); where the interface provides an indication to the administrator that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data (par. 66, lines 11-13); where the policy data store stores IT security policies related to the computing devices (par. 73, lines 14-15); where an administrator defines through the interface a meta IT policy for a security mode of operation (par. 69, lines 9-15); where the defined security mode of operation limits the use of cryptographic algorithms by the devices to those that are specified by the meta IT policy (par. 9, lines 1-6).

7. As to claim 7, Schoen discloses a system where at least one of the plurality of computing devices receives a disable message for disabling the security mode of operation of the one of the plurality of computing devices (par. 73, lines 16-23).

8. As to claim 8, Schoen discloses a computing device utilizing wherein an administrator defines through the interface a meta IT policy for a security mode of operation;. (par. 69, lines 21-32); wherein the defined security mode of operation limits the use of cryptographic algorithms by the devices to those that are specified by the meta IT policy (Schoen; claim 10, lines 2-5).

9. As to claims 9 and 18, Schoen discloses a system where the plurality of computing devices are devices from a group that includes mobile devices, desktop

devices, and combinations thereof (par. 4, lines 14-17; par. 9, lines 1-4; par. 35, lines 2-7).

10. As to claims 11 and 19, the system of Schoen provides security policy related data to device however the system does not disclose a method further comprising the step of displaying the security mode of operation of a computing device by providing a visual indication on a screen of the computing device. In this instance the Examiner notes the teachings of Phillips where Phillips discloses a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, wherein the security mode of operation forces use of one or more cryptographic algorithm. See paragraph 96 of Phillips. Therefore, given the teachings of Phillips, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schoen by employing the well known feature of visually indicating a security level disclosed above by Phillips, for which configuring devices for secure operation will be enhanced.

11. As to claims 12 and 20, the system of Schoen provides security policy related data to device however the system does not disclose a device where the visual indication of the security mode is provided by a security options screen. In this instance the Examiner notes the teachings of Phillips where Phillips discloses a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, wherein the security mode of operation forces use of one or more

cryptographic algorithm. See paragraph 96 of Phillips. Therefore, given the teachings of Phillips, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schoen by employing the well known feature of visually indicating a security level disclosed above by Phillips, for which configuring devices for secure operation will be enhanced.

12. As to claims 13 and 22, Schoen discloses where the security instructions are configured to update the security mode of operation responsive to a change in the configuration data stored on the centralized policy data store (par. 9, lines 3-6),

Schoen does not expressly teach:

wherein a visual indication is provided to the device's user to indicate the updated security mode of operation In this instance the Examiner notes the teachings of Phillips where Phillips discloses a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, wherein the security mode of operation forces use of one or more cryptographic algorithm. See paragraph 96 of Phillips. Therefore, given the teachings of Phillips, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schoen by employing the well known feature of visually indicating a security level disclosed above by Phillips, for which configuring devices for secure operation will be enhanced.

13. As to claim 14, Schoen discloses a device further comprising an administrator interface for changing the configuration data stored on the centralized policy data store. (par. 60, lines 3-5).

14. As to claim 15, Schoen discloses a device where the configuration data stored on the centralized policy data store comprises a plurality of security mode data structures contained within the policy data store (abstract: lines 12-14; par. 33).

15. As to claim 16, Schoen discloses a device where the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices (abstract: lines 12-14; par. 33).

16. As to claims 23, Schoen discloses a computer software stored on one or more non-transitory computer readable media, the computer software comprising program code for carrying out a method (Schoen; claim 12, lines 1-3).

17. Claims 2, 3, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Phillips, as applied to claims 1 and 15, and further in view of Wenocur et al. (US Patent Publication No. 2002/0165912 and Wencour hereinafter).

18. As to claims 2, 3, and 21, although the system disclosed by Schoen shows substantial features of the claimed invention (discussed in the paragraphs above), it

fails to disclose: A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2). A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3). A method where the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 21). However, in this instance the Examiner notes the teachings of prior art Wencour. Wencour discloses a Federal Information Processing Standard (FIPS) mode of operation (par. 254, lines 1-13), a Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) security mode (par. 257, lines 1-7). Therefore given the teachings of Schoen and Phillips, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the system to enhance data security by employing Wencour's data encryption capability utilizing Federal Information Processing Standard (FIPS), Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Flynn Nathan can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/182,827	Applicant(s)/Patent Under Reexamination ADAMS ET AL.	
	Examiner BRYAN WRIGHT	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,490,680	12-2002	Scheidt et al.	713/166
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	
	Filing Date	
	First Named Inventor	Neil P. Adams
	Art Unit	2431
	Examiner Name	Bryan Wright
	Attorney Docket Number	555255-013133

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/B.W./	1	5935248		1999-08-00	Kuroda, Yasutsugu	
/B.W./	2	6202157		2001-03-13	Brownlie et al	
/B.W./	3	6732168		2004-05-04	Bearden et al	
/B.W./	4	6775536		2004-08-00	Geiger et al	
/B.W./	5	7131003		2006-10-00	Lord et al	
/B.W./	6	7317699		2008-01-00	Godfrey et al	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

Receipt date: 07/14/2011 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** **(Not for submission under 37 CFR 1.99)**	Application Number	13182827 - GAU: 2431
	Filing Date	
	First Named Inventor	Neil P. Adams
	Art Unit	2431
	Examiner Name	Bryan Wright
	Attorney Docket Number	555255-013133

/B.W./	1	20020165912		2002-11-00	Wenocur et al	
/B.W./	2	20020186845		2002-12-00	Dutta et al	
/B.W./	3	20030204722		2003-10-00	Schoen et al	
/B.W./	4	20040019807		2004-01-00	Freund, Gregor P.	
/B.W./	5	20050183138		2005-08-00	Phillips et al	
/B.W./	6	20050190764		2005-09-00	Shell et al	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
/B.W/	1	0069120	WO	A1	2000-11-16			□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

Receipt date: 07/14/2011 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** **(Not for submission under 37 CFR 1.99)**	Application Number		13182827 - GAU: 2431
	Filing Date		
	First Named Inventor	Neil P. Adams	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		555255-013133

/B.W./	1	Sems, Marty, "Verifying Identity in a Digital World", August 2000.	□
/B.W./	2	S. Gavrila, et al., "Assigning and Enforcing Security Policies on Handheld Devices", Canadian Information Technology Security Symposium, May 17, 2002, Pages 0-7, XP002440113.	□
/B.W./	3	International Search Report of Application No. PCT/CA2005/000294, date of mailing June 20, 2005, 11 pages.	□
/B.W./	4	Supplementary European Search Report, Issued July 11, 2007 by European Patent Office, for European Patent Application No. 05714536.	□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Bryan Wright/	Date Considered	07/29/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	(configuring near5 device near5 operation and (distribut$5 near3 security) and (security near6 (visual or indication or indicator or indicating or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:58
S2	720	((security near6 (visual or indication or indicator or indicating or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:59
S3	43	S2 and (distribut$9 near5 (security))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:59
S4	218	S2 and ((send or sending or transmit$9 or distribut$9) near5 (security))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:59
S5	132	S4 and (policies or policy or rules)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:00
S6	458	((security near3 (visual or indication or indicator or indicating or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:06
S7	17246	((security near3 (visual or indication or indicator or indicating or display or displaying or displayed)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:06
S8	5768	((security near (visual or indication or indicator or indicating or display or displaying or displayed)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:06
S9	4	(visual near5 security near mode near4 device)	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:07

			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB			

S10	5	(visual near5 security near (mode or settings) near4 device)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:07

S11	6	((visual or displaying) near5 security near (mode or settings) near4 device)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:08

S12	6	security near mode near indicator	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:08

S13	20	security near3 setting near displayed	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:09

S14	0	security near3 modev near displayed	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:10

S15	11	security near3 mode near displayed	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:11

S16	29	security near3 (settings or mode) near displayed	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:12

S17	50	FIPS near3 mode	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:17

S18	3	FIPS near3 mode and visual	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23 00:17

S19	3	deploy near5 security near4 mode near5 devices	US-PGPUB;
			USPAT;
				OR	OFF	2012/04/23 00:19

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S20	4	((deploy or distriute or transfer or download) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:19
S21	4	((deploy$5 or distriute or transfer or download) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:21
S22	4	((deploy$5 or distriut$8 or transfer or download) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:21
S23	5	((deploy$5 or distriut$8 or transfer$6 or download$5) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:21
S24	312	(security near mode near (command or instruction))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:24
S25	0	S24 and security near policies	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:24
S26	37	S24 and policies	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:25
S27	6	deploying near5 security near5 settings	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:25
S28	8	((deploying or distributing) near5 security near5 settings)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:26
S29	2101	((deploying or distributing) near5 security)	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:26

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S30	102	security near5 mode near5 settings	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:27
S31	2398	administrator and security near settings	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:31
S32	641	administrator and security near settings same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:31
S33	0	S32 and (FIFPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:31
S34	10	S32 and (FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:32
S35	5716	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:33
S36	96	S35 and security near5 settings	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:34
S37	1833	((FIPS) and ((encryption or cryptographic) near3 algorithm))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:43
S38	566	S37 and admin$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:43
S39	524	S37 and admin$9 and security and device	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:44

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S40	0	S37 and admin$9 and security and (device same alogrithm)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:44
S41	359	S37 and admin$9 and security and (device same (cryptographic or encryption))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:45
S42	329	S37 and admin$9 and security and (device same (cryptographic or encryption)) and operation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:46
S43	231	S37 and admin$9 and security and (device same (cryptographic or encryption)) and operation and (implement)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:46
S44	40	S37 and admin$9 and security and (device same (cryptographic or encryption) same implement) and operation and (implement)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:46
S45	65	S39 and (indicat$9 same (cryptographic or encryption) near algorithm)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:48
S46	9	(configuring same ((cryptographic or encryption) near4 algorithm) and Fips)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:55
S47	1084	(DES and device and ((cryptographic or encryption) near4 algorithm) and Fips)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:56
S48	354	(DES and device and ((cryptographic or encryption) near4 algorithm) and Fips) and (security) and admin$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:57
S49	84	(DES and device and ((cryptographic or encryption) near4 algorithm) and	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:57

		Fips) and (security) and admin$9 and (policies)	USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB			

5/7/2012 2:35:28 PM
C:\Users\bwright\Documents\EAST\Workspaces\13182827.wsp

Search Notes	**Application/Control No.** 13182827	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN WRIGHT	**Art Unit** 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	5/7/2012	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
Text only search class/subclass 713/166	5/7/2012	Bryan Wright
Automated text search utilizing EAST, WEST, Dervwent, IEEE, NPL, EPO, JPO	5/7/2012	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Index of Claims	**Application/Control No.** 13182827	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN WRIGHT	**Art Unit** 2431

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	05/07/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	13182827
Filing Date	14-Jul-2011
First Named Inventor	Neil Adams
Attorney Docket Number	555255-013133
Title of Invention	System and Method for Configuring Devices for Secure Operations

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Research In Motion Limited	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8010989

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

○ Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

○ Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

○ Applicant(s) status remains as SMALL ENTITY.

● Applicant(s) status remains as other than SMALL ENTITY.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

● An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 40602

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors

○ A joint inventor; all of whom are signing this request

○ The assignee of record of the entire interest that has properly made itself of record pursuant to 37 CFR 3.71

Signature	/FDFeeling/
Name	F. Drexel Feeling

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	13182827
Filing Date:	14-Jul-2011
Title of Invention:	System and Method for Configuring Devices for Secure Operations
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	Stephen D. Scanlon/Debra Pejeau
Attorney Docket Number:	555255-013133

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or terminal disclaimer	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 13182827

Filing Date: 14-Jul-2011

Applicant/Patent under Reexamination: Adams et al.

Electronic Terminal Disclaimer filed on November 2, 2012

☒ APPROVED

This patent is subject to a terminal disclaimer

□ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	14141259
Application Number:	13182827
International Application Number:	
Confirmation Number:	7138
Title of Invention:	System and Method for Configuring Devices for Secure Operations
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	89441
Filer:	Stephen D. Scanlon/Debra Pejeau
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255-013133
Receipt Date:	02-NOV-2012
Filing Date:	14-JUL-2011
Time Stamp:	18:13:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$160
RAM confirmation Number	5355
Deposit Account	501432
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33592 6022ee4cc9b6ffd88c5beeb86c6fc315006b7d71	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30065 d73f98309a583eacf222bb48dae733000f620854	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	63657		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

Attorney Docket No. 555255-013133

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	13/182,827
Filing Date	:	July 14, 2011
For	:	System and Method for Configuring Devices for Secure Operation
Art Unit	:	2431
Examiner	:	Bryan F. Wright
Confirmation No.	:	7138

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Sir:

This paper responds to the non-final Office Action dated August 8, 2012. Please consider the following amendments and remarks. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-013133.

CLAIMS

1. (Original) A system for use in establishing a security-related mode of operation for computing devices, comprising:

a policy data store for storing configuration data related to a plurality of computing devices;

a security mode data structure contained within the policy data store;

wherein the security mode data structure stores a security mode of operation;

wherein the stored security mode of operation is provided to the plurality of computing devices over a network;

wherein the security mode of operation places the plurality of computing devices in a predetermined security mode of operation;

wherein at least one of the plurality of computing devices comprises user interface instructions configured to send an output to a display associated with the one of the plurality of computing devices, the output being configured to comprise a visual indication of the security mode of operation to the user of the one of the plurality of computing devices, wherein the security mode of operation forces use of one or more cryptographic algorithms.

2. (Original) The system of claim 1, wherein the security mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation.

3. (Original) The system of claim 2, wherein the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

4. (Original) The system of claim 1, wherein the security mode data structure comprises a first security mode data structure and a second security mode data structure;

wherein the first security mode data structure includes a first security mode being associated with a first plurality of computing devices;

wherein the second security mode data structure includes a second security mode being associated with a second plurality of computing devices.

5. (Original) The system of claim 4, wherein the first security mode of operation contained in the first data structure is communicated to the first plurality of computing devices in order to place the first plurality of computing devices in the first security mode;

wherein the second security mode of operation contained in the second data structure is communicated to the second plurality of computing devices in order to place the second plurality of computing devices in the second security mode.

6. (Original) The system of claim 5, wherein the providing of the first security mode data structure to the first plurality of devices causes the devices in the first plurality of devices to be placed in a FIPS mode of operation that includes required use of AES encryption;

wherein the providing of the second security mode data structure to the second plurality of devices causes the devices in the second plurality of devices to be placed in a FIPS mode of operation that includes required use of Triple DES (3DES) encryption.

7. (Original) The system of claim 1, wherein at least one of the plurality of computing devices receives a disable message for disabling the security mode of operation of the one of the plurality of computing devices.

8. (Original) The system of claim 1, wherein the policy data store stores IT security policies related to the plurality of computing devices;

wherein an administrator defines through the interface a meta IT policy for a security mode of operation;

wherein the defined security mode of operation limits the use of cryptographic algorithms by the devices to those that are specified by the meta IT policy.

9. (Original) The system of claim 8, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

10. (Original) A computing device utilizing a centralized policy data store to implement a security-related mode of operation, the device comprising:

a communication interface configured to facilitate communication between the centralized policy data store and the computing device; and

a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions;

wherein the processing instructions includes security instructions configured to place the computing device in a security mode of operation responsive to configuration data received from the centralized policy data store via the communication interface;

wherein the computing device comprises user interface instructions configured to send an output to a display associated with the computing device, the output being configured to comprise a visual indication of the security mode of operation to the device's user, wherein the security mode of operation forces use of one or more cryptographic algorithms.

11. (Original) The device of claim 10, wherein the processing instructions further comprise user interface instructions configured to send an output to a display associated with the computing device, the output having a visual indication of the security mode of operation that is visible to the device's user.

12. (Original) The device of claim 11, wherein the visual indication of the security mode is provided by a security options screen.

13. (Original) The device of claim 12, wherein the security instructions are configured to update the security mode of operation responsive to a change in the configuration data stored on the centralized policy data store, wherein a visual indication is provided to the device's user to indicate the updated security mode of operation.

14. (Original) The device of claim 13, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

15. (Original) The device of claim 10, wherein the configuration data stored on the centralized policy data store comprises a plurality of security mode data structures contained within the policy data store.

16. (Original) The device of claim 15, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

17. (Original) A method for use in establishing a security-related mode of operation for a computing device, comprising:

storing a security mode of operation in a policy data store;

sending the stored security mode of operation to the computing device over a network;

wherein the sent security mode of operation places the computing device into a predetermined security-related mode of operation;

wherein the computing device comprises user interface instructions configured to send an output to a display associated with the computing device, the output being configured to comprise a visual indication of the security mode of operation to the device's user, wherein the security mode of operation forces use of one or more cryptographic algorithms.

18. (Original) The method of claim 17, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

19. (Original) The method of claim 17, further comprising the step of displaying the security mode of operation of the computing device by providing a visual indication on a screen of the computing device.

20. (Original) The method of claim 17, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

21. (Original) The method of claim 17, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

22. (Currently Amended) The method of claim 17, wherein the security mode of operation is sent via a ~~A~~ digital signal ~~containing the sent security mode of operation of claim 17~~.

23. (Original) Computer software stored on one or more non-transitory computer readable media, the computer software comprising program code for carrying out a method according to claim 17.

24. (Original) A system for establishing a security-related mode of operation for a computing device, comprising:

means for receiving a security mode of operation from a server, the server comprising a security mode data structure comprising security mode data for a plurality of computing devices;

means for entering the security mode of operation received from the server, wherein the means for entering includes means for forcing use of AES or 3DES;

means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device, wherein the security mode of operation forces use of one or more cryptographic algorithms.

REMARKS

This paper responds to the non-final Office Action dated August 8, 2012. Claims 1-24 are pending in the instant application and stand rejected. Claims 1, 10, 17, and 24 stand rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 8,010,989. Claim 22 stands rejected under 35 U.S.C. 101 for being directed to non-statutory subject matter. Claims 1, 4-20, and 22-24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen et al. (U.S. Publication No. 2003/0204722) in view of Phillips et al. (U.S. Publication No. 2005/0183138) and further in view of Scheidt et al. (U.S. Patent No. 6,490,680). Claims 2, 3, and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen et al. in view of Phillips et al. and further in view of Wenocur et al. (U.S. Publication No. 2002/0165912).

An eTerminal Disclaimer has been filed to obviate the claim rejections on the ground of nonstatutory obviousness-type double patenting. Claim 22 has been amended to obviate the rejection of claim 22 under 35 U.S.C. 101 for being directed to non-statutory subject matter. The assignee traverses the rejections of the pending claims under 35 U.S.C. 103(a).

In view of the foregoing amendments and the remarks that follow, the assignee requests reconsideration of this application.

Nonstatutory Obviousness-type Double Patenting Rejection

Claims 1, 10, 17, and 24 stand rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 8,010,989. An eTerminal Disclaimer has been filed to obviate these claim rejections. In view of the eTerminal Disclaimer, it is respectfully requested that these claim rejections be withdrawn.

Non-statutory Subject Matter Rejection

Claim 22 stands rejected under 35 U.S.C. 101 for being directed to non-statutory subject matter. Claim 22 has been amended to obviate this rejection. Claim 22 now recites: "The method of claim 17, wherein the security mode of operation is sent via a digital signal." In view of the claim amendment, it is respectfully requested that this claim rejection be withdrawn.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 4-20, and 22-24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen et al. in view of Phillips et al. and further in view of Scheidt et al. Claims 2, 3, and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen et al. in view of Phillips et al. and further in view of Wenocur et al. These rejections are respectfully traversed.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. The Office Action admits that the combination of Schoen and Phillips fails to teach or disclose the following claim features recited in claim 1:

> where the security mode data structure stores a security mode of operation;
>
> wherein the security mode of operation forces use of one or more security algorithms; and
>
> where the security mode of operation places the computing devices in a predetermined security mode of operation.

The Office Action, however, relies on Scheidt, and Column 8 of Scheidt in particular, for disclosing these claim features.

It is respectfully submitted that neither Scheidt alone nor the combination of Scheidt with Schoen and Phillips teaches these claim features. The cited section of Scheidt relates to a "Constructive Key Management System" that has a "multi-tiered infrastructure to manage the secure distribution of information." Scheidt at Col. 7, lines 29-31. The three tiers disclosed in the cited section include: "the Policy Manager [which] serves as the central authority for generating encryption keys and managing the encryption algorithms used by a particular domain residing on the computer network" (Col. 7, lines 44-48); "the Credential Manager Process" which "implement[s] a system of access to information that is based on the roles maintained by user within an organization" (Col. 8, lines 2-6); and "the User Session, which performs the function of encrypting and decrypting objects for transmission through the computer network by individual users." (Col. 8, lines 10-13).

The applicant submits that Col. 8 of Scheidt fails to disclose (i) either a security mode data structure or a security mode data structure that stores a security mode of operation for a computing device; (ii) a security mode of operation that forces the use by the computing devices of one or more security algorithms; and fails to disclose (iii) a security mode of operation that places the computing devices in a predetermined security mode of operation. Because the cited references, singly or in combination, fail to disclose the above-noted features of claim 1, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

Independent claims 10, 17, and 24 recite similar features as claim 1. These claims are allowable for at least the same reasons as offered for claim 1.

Assignee at this time has not provided arguments in support of the patentability of certain dependent claims. It is respectfully submitted that because the independent claims are in condition for allowance, the dependent claims which depend directly or indirectly therefrom are also in condition for allowance. However, assignee reserves the right to argue the patentability of certain of the dependent claims in the instant application at a future time, should that become necessary.

CONCLUSION

For the foregoing reasons, the assignee respectfully submits that the pending claims are allowable. Therefore, the assignee respectfully requests that the examiner pass this case to issuance.

Respectfully submitted,
By:
F. D. Feeling

F. Drexel Feeling
Reg. No. 40,602
JONES DAY
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-7199

Electronic Acknowledgement Receipt

EFS ID:	14141344
Application Number:	13182827
International Application Number:	
Confirmation Number:	7138
Title of Invention:	System and Method for Configuring Devices for Secure Operations
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	89441
Filer:	Stephen D. Scanlon/Debra Pejeau
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255-013133
Receipt Date:	02-NOV-2012
Filing Date:	14-JUL-2011
Time Stamp:	18:18:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		013133_Amendment.pdf	115459 1ce763959d71b00142ce157d57b54c9c39b2de90	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	12
Warnings:			
Information:			
	Total Files Size (in bytes):	115459	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/182,827	Filing Date 07/14/2011	□ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY □		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
□ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**11/02/2012**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0	X $ =		OR	X $62=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $250=	0
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/LYNNELL JOHNSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

89441 7590 01/17/2013

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 01/17/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/182,827	07/14/2011	Neil P. Adams	555255-013133	7138

TITLE OF INVENTION: SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	04/17/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

89441 7590 01/17/2013

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/182,827	07/14/2011	Neil P. Adams	555255-013133	7138

TITLE OF INVENTION: SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	04/17/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
WRIGHT, BRYAN F	2431	726-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________

2____________________

3____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ______________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ____________________ Date ____________________

Typed or printed name ____________________ Registration No. ____________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/182,827	07/14/2011	Neil P. Adams	555255-013133	7138

89441 7590 01/17/2013

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 01/17/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 13/182,827	**Applicant(s)** ADAMS ET AL.	
	Examiner BRYAN WRIGHT	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 11/2/2012*.

2. □ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-24*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. □ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. □ Other _____.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

REASONS FOR ALLOWANCE

1. The terminal disclaimer filed on 11/2/2012 disclaiming the terminal portion of any patent granted on this application has been reviewed and is accepted. The terminal disclaimer has been recorded.

2. Applicant's invention configures a plurality of devices into a secure mode according to an IT policy. The secure mode is a cryptographic security mode of operation that forces the use of one or more cryptographic algorithms. Accordingly, the Examiner finds applicant's remarks filed on 11/2/2012 for patentability over the cited prior art references of Schoen et al. (US Patent Publication No. 2003/0204722), Phillps et al. (US Patent Publication No. 2005/0183138) and Scheidt et al. (US Patent No. 6,490,680) and Scheidt hereinafter) pertaining to the above noted inventive feature, to be persuasive. More specifically, the Examiner concurs with applicant's stated opinion that the cited prior art fails to disclose, "…(ii) a security mode of operation that forces the use by the computing devices of one or more security algorithms; and fails to disclose (iii) a security mode of operation that places the computing devices in a predetermined security mode of operation".

Additionally the Examiner notes that applicant's Independent claims 10, 17, and 24 recite similar features and are therefore allowable of the cited prior art.

3. The Examiner notes for the record the teachings of prior art reference Nehushtan (US Patent Publication No. 2005/0197099). The Examiner contends that the above

reference was obtained as a result of an updated prior art and interference search and has not been relied upon in a formal rejection. The Examiner notes Nehushtan's teachings in this instance because Nehushtan discloses holding device specific information for a plurality of devices to create device specific security setting for a particular data protection mode on the plurality of device. The Examiner notes that while the applicant discloses a similar feature, the Examiner contends that Nehushtan does not disclose or make obvious applicant's claim limitation element of: "…a security mode of operation that forces the use by the computing devices of one or more security algorithms…".

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

Accordingly, Claims 1-24 are allowed.

Response to Arguments

The Examiner withdraws rejection made under 35 USC § 101 for claim 22 in view of applicant's claim amendment.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Flynn Nathan can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/182,827	Applicant(s)/Patent Under Reexamination ADAMS ET AL.	
	Examiner BRYAN WRIGHT	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0197099	09-2005	Nehushtan, Rafi	455/410
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No. 13182827	Applicant(s)/Patent Under Reexamination ADAMS ET AL.
	Examiner BRYAN WRIGHT	Art Unit 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	5/7/2012	Bryan Wright
726	1	1/12/2013 (Updated Search)	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
Text only search class/subclass 713/166	5/7/2012	Bryan Wright
Automated text search utilizing EAST, WEST, Dervwent, IEEE, NPL, EPO, JPO	5/7/2012	Bryan Wright
Limited text search class/subclass 726/1-4, 726/11, 726/22-28, 713/165-188, 713/193, 455/411, 380/37-40, 380/270, 380/277	1/12/2013	Bryan Wright
Automated text search utilizing EAST, WEST, Dervwent, IEEE, NPL, EPO, JPO	1/12/2013	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	1-4, 11, 22, 27, 28	1/12/2013	Bryan Wright
713	165, 167, 188, 189, 193, 168	1/12/2013	Bryan Wright
455	410, 411	1/12/2013	Bryan Wright
380	37, 42, 270, 277	1/12/2013	Bryan Wright

Interference Search Noted /B.W./ Examiner.Art Unit 2431	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13182827	ADAMS ET AL.
	Examiner	**Art Unit**
	BRYAN WRIGHT	2431

ORIGINAL	
CLASS	**SUBCLASS**
455	410

CROSS REFERENCE(S)

CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
726	1	2	3	4	11
726	22	27	28		
713	165	167	188	189	193
713	168				
455	411				
380	277	270	37	42	

INTERNATIONAL CLASSIFICATION

CLAIMED					**NON-CLAIMED**				
H	0	4	M	1 / 66 (2006.0)	H	0	4	M	1 / 66 (2006.0)
H	0	4	M	1 / 68 (2006.0)	H	0	4	M	1 / 68 (2006.0)
H	0	4	M	3 / 16 (2006.0)	H	0	4	M	3 / 16 ()

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☒ **T.D.** ☐ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6	22	22												
7	7	23	23												
8	8	24	24												
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

/BRYAN WRIGHT/ Examiner.Art Unit 2431 (Assistant Examiner)	1/11/2013 (Date)	**Total Claims Allowed:** 24	
(Primary Examiner)	(Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office Part of Paper No. 20130111

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	(configuring near5 device near5 operation and (distribut$5 near3 security) and (security near6 (visual or indication or indicator or indicating or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:58
S2	720	((security near6 (visual or indication or indicator or indicating or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:59
S3	43	S2 and (distribut$9 near5 (security))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:59
S4	218	S2 and ((send or sending or transmit$9 or distribut$9) near5 (security))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/22 23:59
S5	132	S4 and (policies or policy or rules)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:00
S6	458	((security near3 (visual or indication or indicator or indicating or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:06
S7	17246	((security near3 (visual or indication or indicator or indicating or display or displaying or displayed)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:06
S8	5768	((security near (visual or indication or indicator or indicating or display or displaying or displayed)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:06
S9	4	(visual near5 security near mode near4 device)	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:07

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S10	5	(visual near5 security near (mode or settings) near4 device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:07
S11	6	((visual or displaying) near5 security near (mode or settings) near4 device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:08
S12	6	security near mode near indicator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:08
S13	20	security near3 setting near displayed	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:09
S14	0	security near3 modev near displayed	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:10
S15	11	security near3 mode near displayed	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:11
S16	29	security near3 (settings or mode) near displayed	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:12
S17	50	FIPS near3 mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:17
S18	3	FIPS near3 mode and visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:17
S19	3	deploy near5 security near4 mode near5 devices	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:19

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S20	4	((deploy or distriute or transfer or download) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:19
S21	4	((deploy$5 or distriute or transfer or download) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:21
S22	4	((deploy$5 or distriut$8 or transfer or download) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:21
S23	5	((deploy$5 or distriut$8 or transfer$6 or download$5) near5 security near4 mode near5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:21
S24	312	(security near mode near (command or instruction))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:24
S25	0	S24 and security near policies	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:24
S26	37	S24 and policies	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:25
S27	6	deploying near5 security near5 settings	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:25
S28	8	((deploying or distributing) near5 security near5 settings)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:26
S29	2101	((deploying or distributing) near5 security)	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:26

			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB			

S30	102	security near5 mode near5 settings	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:27

S31	2398	administrator and security near settings	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:31

S32	641	administrator and security near settings same device	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:31

S33	0	S32 and (FIFPS)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:31

S34	10	S32 and (FIPS)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:32

S35	5716	(FIPS)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:33

S36	96	S35 and security near5 settings	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:34

S37	1833	((FIPS) and ((encryption or cryptographic) near3 algorithm))	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:43

S38	566	S37 and admin$9	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/04/23
						00:43

S39	524	S37 and admin$9 and security and device	US-PGPUB;
			USPAT;
				OR	OFF	2012/04/23
						00:44

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S40	0	S37 and admin$9 and security and (device same alogrithm)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:44
S41	359	S37 and admin$9 and security and (device same (cryptographic or encryption))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:45
S42	329	S37 and admin$9 and security and (device same (cryptographic or encryption)) and operation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:46
S43	231	S37 and admin$9 and security and (device same (cryptographic or encryption)) and operation and (implement)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:46
S44	40	S37 and admin$9 and security and (device same (cryptographic or encryption) same implement) and operation and (implement)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:46
S45	65	S39 and (indicat$9 same (cryptographic or encryption) near algorithm)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:48
S46	9	(configuring same ((cryptographic or encryption) near4 algorithm) and Fips)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:55
S47	1084	(DES and device and ((cryptographic or encryption) near4 algorithm) and Fips)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:56
S48	354	(DES and device and ((cryptographic or encryption) near4 algorithm) and Fips) and (security) and admin$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/04/23 00:57
S49	84	(DES and device and ((cryptographic or encryption) near4 algorithm) and	US-PGPUB; USPAT;	OR	OFF	2012/04/23 00:57

		Fips) and (security) and admin$9 and (policies)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S62	1	"11065901"	USPAT	OR	OFF	2012/05/07 14:51

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"11065901"	US-PGPUB; USPAT; UPAD	OR	OFF	2013/01/12 21:42
S50	8412	security near5 mode	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:32
S51	14	security near5 mode near6 (plurality or multiple) near5 devices	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:33
S52	225	security near5 mode near5 devices	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:42
S53	53	security near5 mode near5 devices and policy	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:42
S54	104	security near5 (parameter or setting or mode) near5 devices and policy	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:46
S55	979	configuring near5 device near5 operation	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:48
S56	1	configuring near5 device near5 operation and (distributing near3 security)	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:49
S57	12	configuring near5 device near5 operation and (distribut$5 near3 security)	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:50
S58	11	(configuring near5 device near5 operation and (distribut$5 near3 security) and (visual or indicat$9 or display or displaying))	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:54
S59	7	(configuring near5 device near5 operation and (distribut$5 near3 security) and (security same (visual or indicat$9 or display or displaying)))	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:54
S60	10	(configuring near5 device near5 operation and (distribut$5 near3 security) and (security near6 (visual or indicat$9 or display or displaying or displayed) (settings)))	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:57

S61	0	(configuring near5 device near5 operation and (distribut$5 near3 security) and (security near6 (visual or indicat$9 or display or displaying or displayed) same (settings)))	US-PGPUB; USPAT; UPAD	OR	OFF	2012/04/22 23:57
S63	1	"13182827"	US-PGPUB; USPAT; UPAD	OR	OFF	2012/07/03 15:16
S64	0	S63 and means	US-PGPUB; USPAT; UPAD	OR	OFF	2012/07/03 15:16
S65	0	S63 and mean	US-PGPUB; USPAT; UPAD	OR	OFF	2012/07/03 15:16
S66	4	"20030204722" "20050183138" ("6490680").pn.	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/08 21:20
S67	0	S66 and security near mode	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/08 21:20
S68	3	S66 and mode	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/08 21:21
S69	48	(configure or configuring) same security same mode same (multiple or plurality) same device	US-PGPUB; USPAT; UPAD	OR	OFF	2013/01/11 12:31
S70	1	(configure or configuring) same security same mode same (multiple or plurality) near device	US-PGPUB; USPAT; UPAD	OR	OFF	2013/01/11 12:32
S71	6	(configure or configuring) same security same mode same (multiple or plurality) near4 device	US-PGPUB; USPAT; UPAD	OR	OFF	2013/01/11 12:33

1/12/2013 10:30:32 PM
C:\Users\bwright\Documents\EAST\Workspaces\13182827.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7138

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/182,827	07/14/2011 **RULE**	726	2431	555255-013133

APPLICANTS

Neil P. Adams, Waterloo, CANADA;
Michael K. Brown, Waterloo, CANADA;
Michael S. Brown, Waterloo, CANADA;
Michael G. Kirkup, Waterloo, CANADA;
Herbert A. Little, Waterloo, CANADA;
David Victor MacFarlane, Waterloo, CANADA;
Ian M. Robertson, Waterloo, CANADA;

** **CONTINUING DATA** *************************

This application is a CON of 11/065,901 02/25/2005 PAT 8,010,989
which claims benefit of 60/567,137 04/30/2004

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** **
07/25/2011

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed □ Yes □ No 35 USC 119(a-d) conditions met □ Yes □ No Verified and Acknowledged ____________ Examiner's Signature	□ Met after Allowance ______ Initials	CANADA	10	24	4

ADDRESS

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114
UNITED STATES

TITLE

System and Method for Configuring Devices for Secure Operations

FILING FEE RECEIVED 1518	FEES: Authority has been given in Paper No.___________ to charge/credit DEPOSIT ACCOUNT No.___________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue) □ Other _______________ □ Credit

Index of Claims	**Application/Control No.** 13182827	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN WRIGHT	**Art Unit** 2431

✓	**Rejected**		-	**Cancelled**		N	**Non-Elected**		A	**Appeal**
=	**Allowed**		÷	**Restricted**		I	**Interference**		O	**Objected**

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☒ **T.D.** ☐ **R.1.47**

CLAIM		**DATE**								
Final	Original	05/07/2012	01/11/2013							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	✓	=							
9	9	✓	=							
10	10	✓	=							
11	11	✓	=							
12	12	✓	=							
13	13	✓	=							
14	14	✓	=							
15	15	✓	=							
16	16	✓	=							
17	17	✓	=							
18	18	✓	=							
19	19	✓	=							
20	20	✓	=							
21	21	✓	=							
22	22	✓	=							
23	23	✓	=							
24	24	✓	=							

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

89441 7590 01/17/2013

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Debra Pejeau	(Depositor's name)
Debra Pejeau	(Signature)
April 16, 2013	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/182,827	07/14/2011	Neil P. Adams	555255-013133	7138

TITLE OF INVENTION: SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	04/17/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
WRIGHT, BRYAN F	2431	726-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Jones Day
2 ____________
3 ____________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Research In Motion Limited	Waterloo, Canada

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual ☒ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies ____________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 501432 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. □ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ____________ Date 4/9/2013

Typed or printed name F. Drexel Feeling Registration No. 40602

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	13182827
Filing Date:	14-Jul-2011
Title of Invention:	SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	Joseph McGowan Sauer/Debra Pejeau
Attorney Docket Number:	555255-013133

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	1780	1780
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2080**

Electronic Acknowledgement Receipt

EFS ID:	15526133
Application Number:	13182827
International Application Number:	
Confirmation Number:	7138
Title of Invention:	SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS
First Named Inventor/Applicant Name:	Neil P. Adams
Customer Number:	89441
Filer:	Joseph McGowan Sauer/Debra Pejeau
Filer Authorized By:	Joseph McGowan Sauer
Attorney Docket Number:	555255-013133
Receipt Date:	16-APR-2013
Filing Date:	14-JUL-2011
Time Stamp:	10:23:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2080
RAM confirmation Number	9146
Deposit Account	501432
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	013133.pdf	99646 ad28b4b9db043f52887d4a59a51cc837c69 79f96	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32004 bd16a1b70f0ae3f0a8a92f263cd275d27dffc e6e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	131650	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/182,827	05/14/2013	8442489	555255-013133	7138

89441 7590 04/24/2013

Jones Day (BlackBerry) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Neil P. Adams, Waterloo, CANADA;
Michael K. Brown, Waterloo, CANADA;
Michael S. Brown, Waterloo, CANADA;
Michael G. Kirkup, Waterloo, CANADA;
Herbert A. Little, Waterloo, CANADA;
David Victor MacFarlane, Waterloo, CANADA;
Ian M. Robertson, Waterloo, CANADA;

IR103 (Rev. 10/09)