PTO/SB/05 (08-03)
Approved for use through 07/31/2006. 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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	555255-012798
First Inventor	Neil P. Adams
Title	System and Method for Configuring Devices for Secure Operations
Express Mail Label No.	EV 302226610 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

1. ☑ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. □ Applicant claims small entity status. See 37 CFR 1.27.
3. ☑ Specification [*Total Pages* 27]
   (preferred arrangement set forth below)
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☑ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 10]
5. Oath or Declaration [*Total Sheets* ______]
   a. □ Newly executed (original or copy)
   b. □ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. □ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. □ Application Data Sheet. See 37 CFR 1.76
7. □ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. □ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. □ CD-ROM or CD-R (2 copies); or
      ii. □ Paper
   c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ Assignment Papers (cover sheet & document(s))
10. □ 37 CFR 3.73(b) Statement *(when there is an assignee)* □ Power of Attorney
11. □ English Translation Document *(if applicable)*
12. □ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations
13. □ Preliminary Amendment
14. ☑ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. □ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. □ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☑ Other: Claims priority on US Provisional 60/567,137 Filed 4/30/2004

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No.: ______

Prior application information: *Examiner* ______ *Art Unit:* ______

For CONTINUATION OF DIVISIONAL APPS only; The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

□ Customer Number: ______ *OR* ☑ Correspondence address below

Name	John V. Biernacki, Esq.				
Address	JONES DAY North Point, 901 Lakeside Avenue				
City	Cleveland	State	Ohio	Zip Code	44114
Country	USA	Telephone	(216) 586-3939	Fax	(216)579-0212

Name (Print/Type)	John V. Biernacki	Registration No. (Attorney/Agent)	40,511
Signature	John Biernacki	Date	02/25/2005

This collection of information is required by 37 CFR 1.53(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 1.14. 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: Mail Stop Patent Application, 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/17 (12-04v2)
Approved for use through 07/31/2006. 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

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 1,300.00

Complete if Known

Application Number	
Filing Date	February 25, 2005
First Named Inventor	Neil P. Adams
Examiner Name	
Art Unit	
Attorney Docket No.	555255012798

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order □ None □ Other (please identify): ____________

☑ Deposit Account Deposit Account Number: 501432 (555255012798) Deposit Account Name: Jones Day

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below
□ Charge fee(s) indicated below, **except for the filing fee**
☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17
☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	1000
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

		Small Entity
Fee Description	Fee ($)	Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
22	- 20 or HP =	2	x	50	=	100

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
4	- 3 or HP =	1	x	200	=	200

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims

Fee ($)	Fee Paid ($)
	0

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), 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).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof		Fee ($)		Fee Paid ($)
37	- 100 =	0	/ 50 =	0 (round up to a whole number)	x	250	=	0

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	0
Other (e.g., late filing surcharge):	0

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 40,511	Telephone 216/586-7747
Name (Print/Type)	John V. Biernacki		Date 02/25/2005

This collection of information is required by 37 CFR 1.136. 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 30 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/05 (08-03)
Approved for use through 07/31/2006. 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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	555255-012798
First Inventor	Neil P. Adams
Title	System and Method for Configuring Devices for Secure Operations
Express Mail Label No.	EV 302226610 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

1. ☑ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. □ Applicant claims small entity status.
See 37 CFR 1.27.
3. ☑ Specification [*Total Pages* 27]
(preferred arrangement set forth below)
- Descriptive title of the invention
- Cross Reference to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to sequence listing, a table, or a computer program listing appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings *(if filed)*
- Detailed Description
- Claim(s)
- Abstract of the Disclosure
4. ☑ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 10]
5. Oath or Declaration [*Total Sheets* ________]
a. □ Newly executed (original or copy)
b. □ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 18 completed)
i. □ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. □ Application Data Sheet. See 37 CFR 1.76
7. □ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. □ Computer Readable Form (CRF)
b. Specification Sequence Listing on:
i. □ CD-ROM or CD-R (2 copies); or
ii. □ Paper
c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ Assignment Papers (cover sheet & document(s))
10. □ 37 CFR 3.73(b) Statement *(when there is an assignee)* □ Power of Attorney
11. □ English Translation Document *(if applicable)*
12. □ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations
13. □ Preliminary Amendment
14. ☑ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
15. □ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. □ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☑ Other: Claims priority on US Provisional 60/567,137 Filed 4/30/2004

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No.:

Prior application information: Examiner ________________ *Art Unit:* ________________

For CONTINUATION OF DIVISIONAL APPS only; The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

□ Customer Number: ________ *OR* ☑ Correspondence address below

Name	John V. Biernacki, Esq.				
Address	JONES DAY North Point, 901 Lakeside Avenue				
City	Cleveland	*State*	Ohio	*Zip Code*	44114
Country	USA	*Telephone*	(216) 586-3939	*Fax*	(216)579-0212

Name (Print/Type)	John V. Biernacki	*Registration No. (Attorney/Agent)*	40,511
Signature	John Biernacki	*Date*	02/25/2005

This collection of information is required by 37 CFR 1.53(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 1.14. 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: Mail Stop Patent Application, 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/17 (12-04v2)
Approved for use through 07/31/2006. 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

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 1,300.00

Complete if Known

Application Number	
Filing Date	February 25, 2005
First Named Inventor	Neil P. Adams
Examiner Name	
Art Unit	
Attorney Docket No.	555255012798

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order □ None □ Other (please identify):

☑ Deposit Account Deposit Account Number: 501432 (555255012798) Deposit Account Name: Jones Day

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below

□ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17

☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	**Fee ($)**	**Fee ($)**	**Fee ($)**	**Fee ($)**	**Fee ($)**	**Fee ($)**	**Fees Paid ($)**
Utility	300	150	500	250	200	100	1000
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

		Small Entity
Fee Description	**Fee ($)**	**Fee ($)**
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims		**Extra Claims**		**Fee ($)**		**Fee Paid ($)**
22	- 20 or HP =	2	x	50	=	100

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		**Extra Claims**		**Fee ($)**		**Fee Paid ($)**
4	- 3 or HP =	1	x	200	=	200

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims

Fee ($)	**Fee Paid ($)**
	0

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), 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).

Total Sheets		**Extra Sheets**		**Number of each additional 50 or fraction thereof**		**Fee ($)**		**Fee Paid ($)**
37	- 100 =	0	/ 50 =	0 (round up to a whole number)	x	250	=	0

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	0
Other (e.g., late filing surcharge):	0

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	40,511	Telephone	216/586-7747
Name (Print/Type)	John V Biernacki			Date	02/25/2005

This collection of information is required by 37 CFR 1.136. 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 30 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.

SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of commonly assigned United States Provisional Application having serial number 60/567,137, filed April 30, 2004, entitled "SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATION," which is hereby incorporated by reference in its entirety for all purposes.

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.

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 computing devices over a network;

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

wherein the 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.

2. The system of claim 1, wherein the secure 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 1, wherein 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;

wherein 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;

wherein the policy data store stores IT security policies related to the 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.

7. The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. 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 secure mode of operation responsive to configuration data received from the centralized policy data store via the communication interface.

9. The device of claim 8, 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.

10. The system of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. The device of claim 10, 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.

12. The device of claim 11, wherein a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store.

13. The device of claim 8, 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.

14. The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

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

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

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

wherein the sent security mode of operation places the computing devices into one or more predetermined security-related modes of operation.

16. The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. The method of claim 15, 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.

18. The method of claim 15, further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation.

19. The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. A digital signal containing the sent security mode of operation of claim 15.

21. Computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15.

22. 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.

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.

PATENT APPLICATION FEE DETERMINATION RECORD
Effective December 8, 2004

11065901

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	22	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	22 minus 20=	* 2
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		□

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE □ OR OTHER THAN SMALL ENTITY

RATE	FEE		RATE	FEE
BASIC FEE	150.00	OR	BASIC FEE	300.00
X$ 25=		OR	X$50=	100
X100=		OR	X200=	200
+180=		OR	+360=	
TOTAL		OR	TOTAL	606

CLAIMS AS AMENDED - PART II

SMALL ENTITY OR OTHER THAN SMALL ENTITY

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. 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.

PATENT APPLICATION SERIAL NO. ____________________

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

```
03/02/2005 EHAILE1  00000007 501432   11065901

01 FC:1011        300.00 DA
02 FC:1111        500.00 DA
03 FC:1311        200.00 DA
04 FC:1201        200.00 DA
05 FC:1202        100.00 DA
```

*U.S. Government Printing Office: 2002 — 489-267/69033

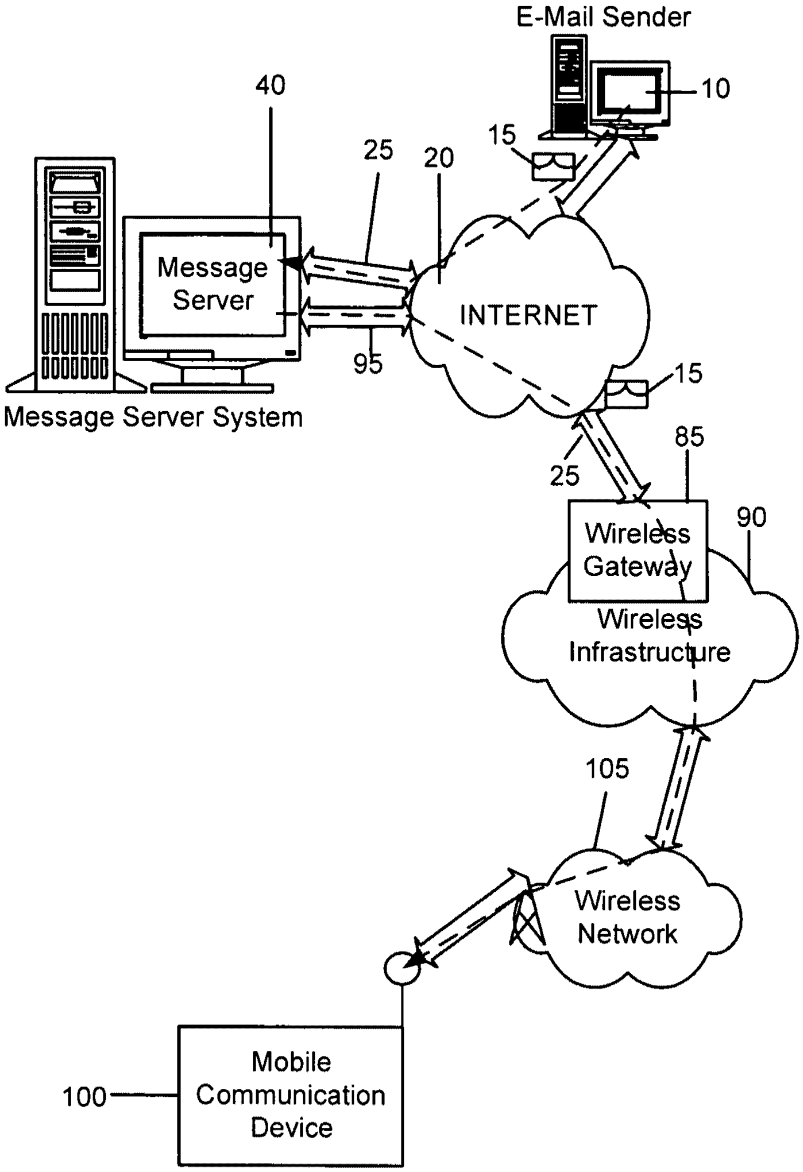

E-Mail Sender
10
40
25
20
15
Message Server
INTERNET
95
Message Server System
15
85
25
Wireless Gateway
90
Wireless Infrastructure
105
Wireless Network
Mobile Communication Device
100

FIG. 1

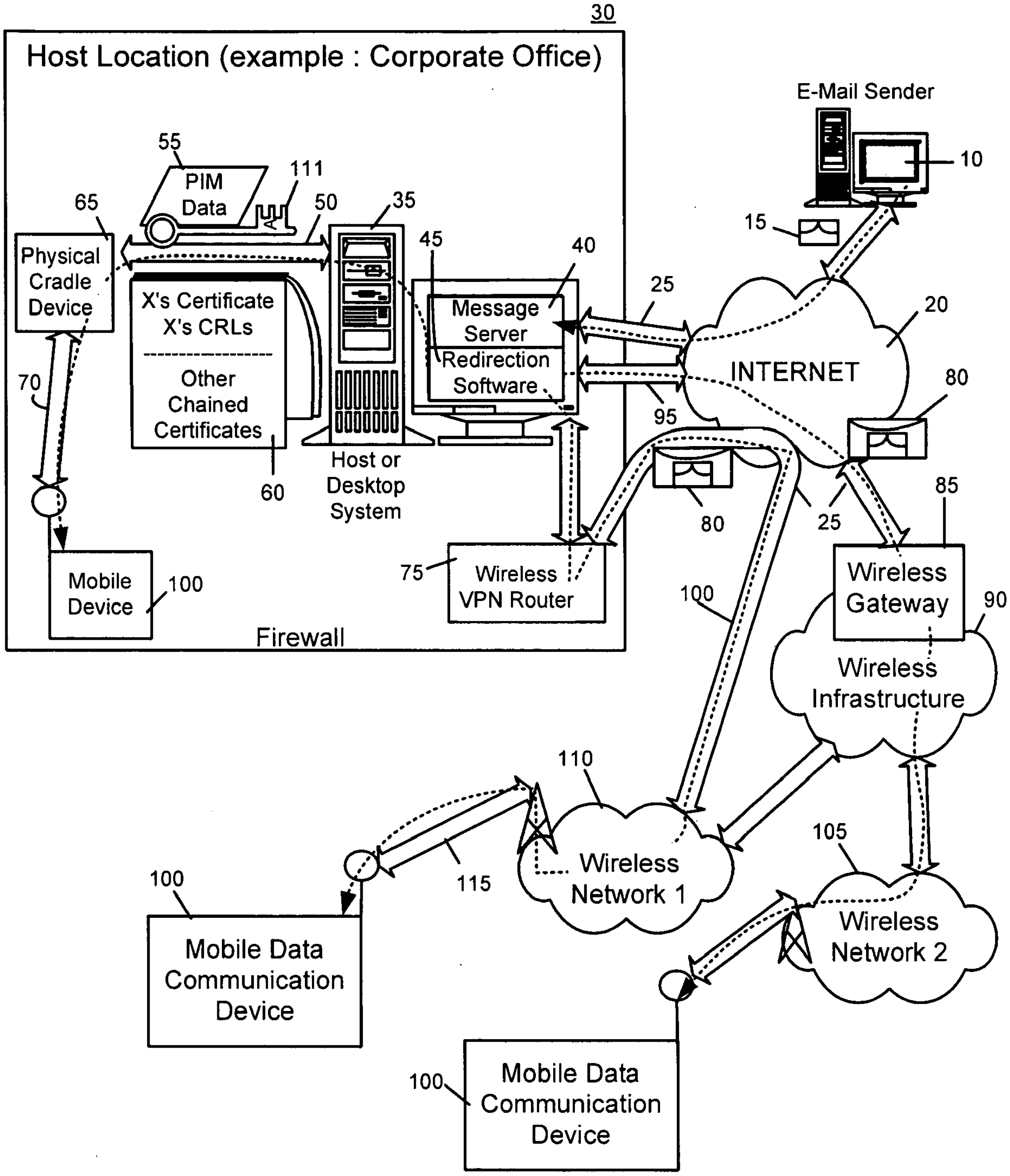

30
Host Location (example : Corporate Office)
55
PIM Data
111
65
50
35
Physical Cradle Device
45
40
X's Certificate
X's CRLs
Other Chained Certificates
Message Server
Redirection Software
70
60
Host or Desktop System
75
Wireless VPN Router
Mobile Device
100
Firewall
E-Mail Sender
10
15
25
20
INTERNET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

FIG. 2

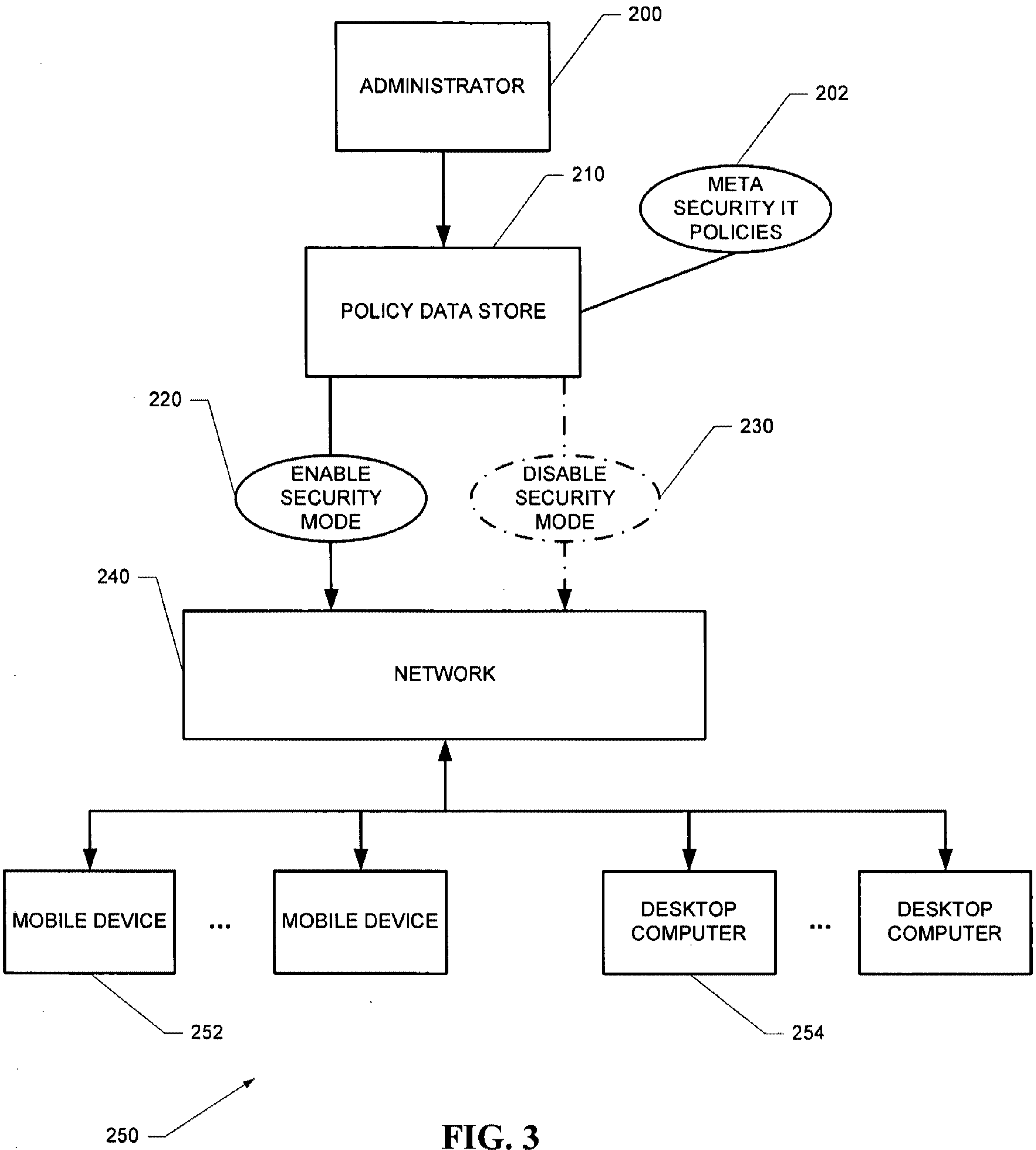

200
ADMINISTRATOR
202
META SECURITY IT POLICIES
210
POLICY DATA STORE
220
ENABLE SECURITY MODE
230
DISABLE SECURITY MODE
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
254
250

FIG. 3

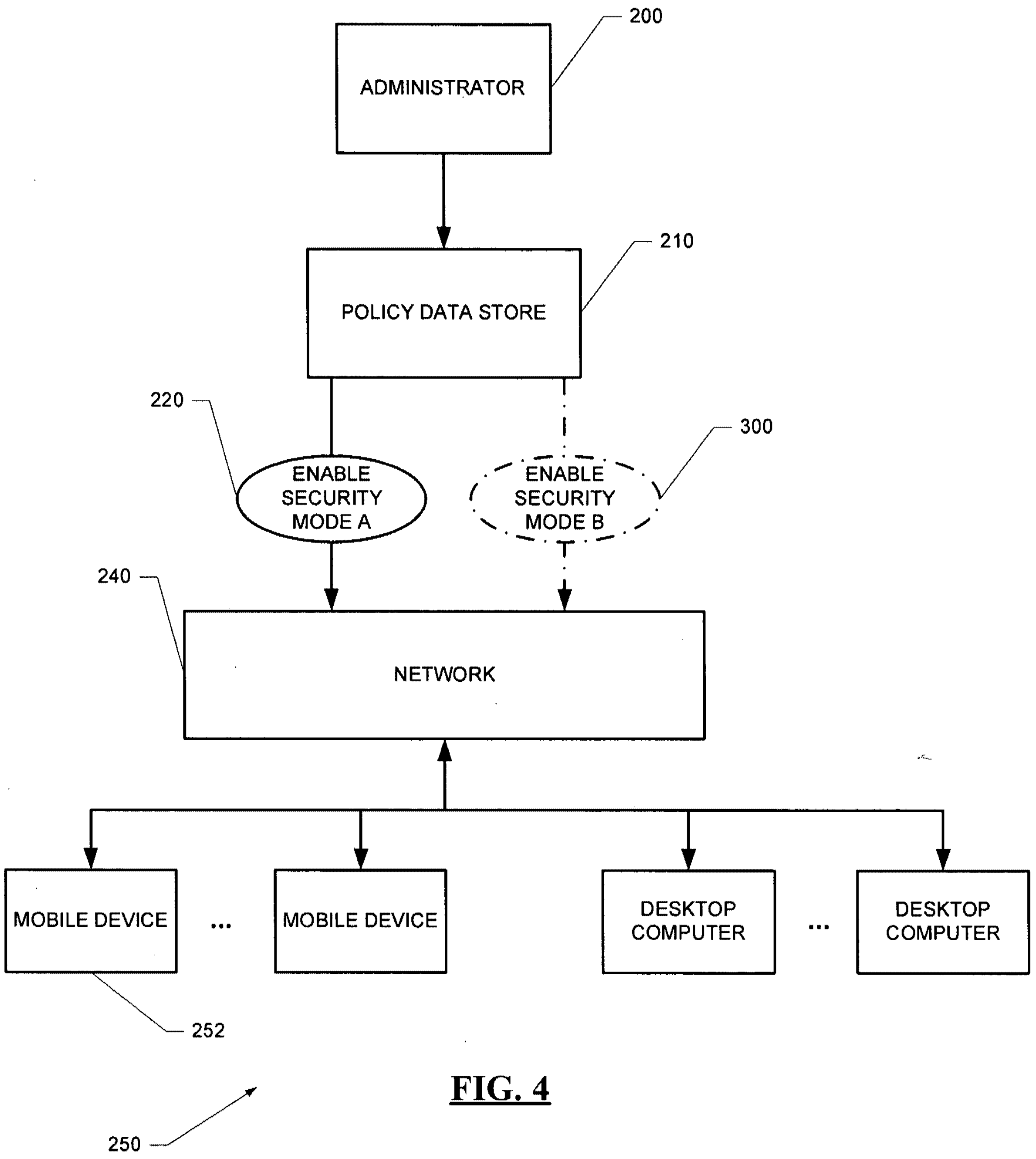

200
ADMINISTRATOR
210
POLICY DATA STORE
220
300
ENABLE SECURITY MODE A
ENABLE SECURITY MODE B
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
250

FIG. 4

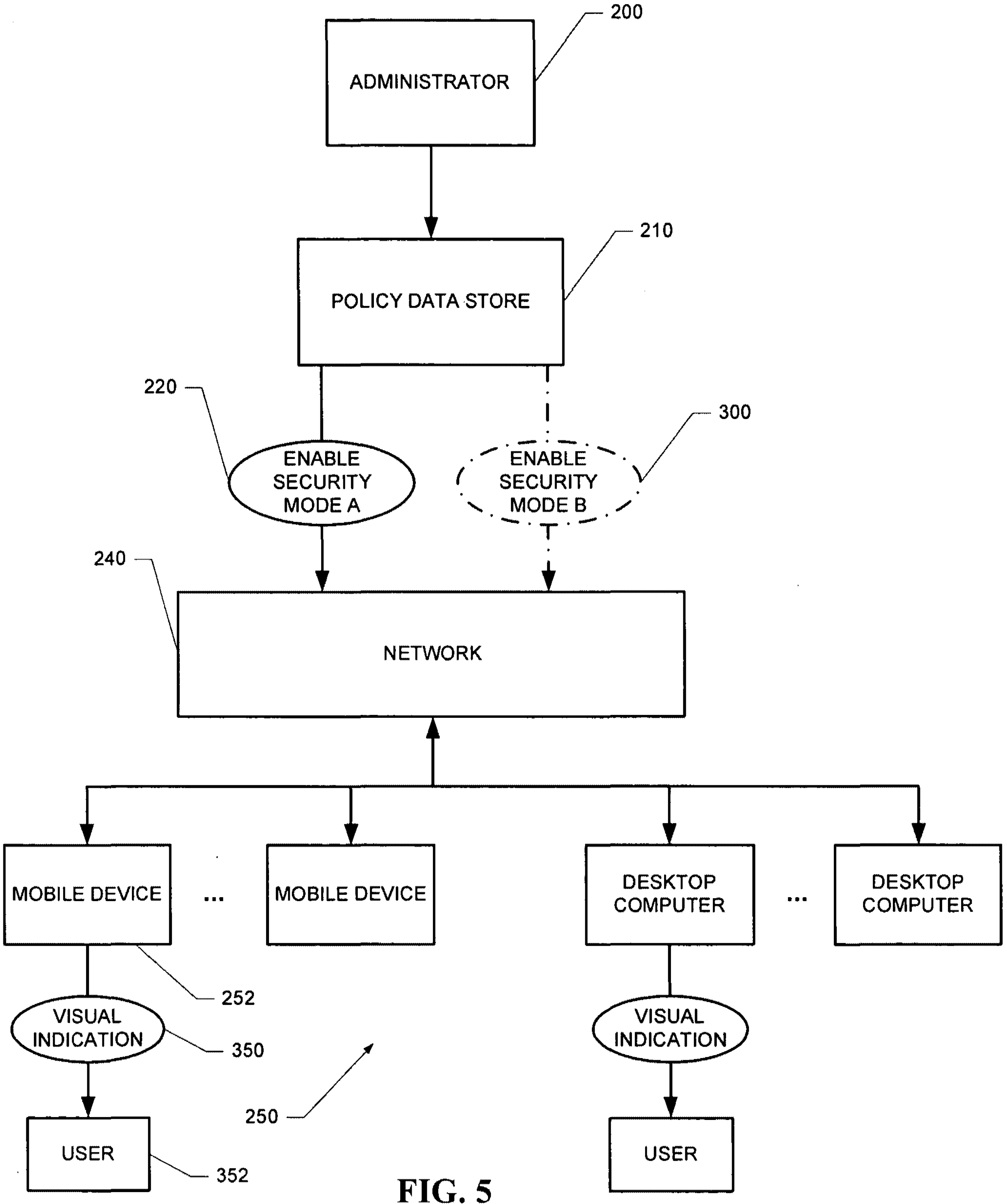

200
ADMINISTRATOR
210
POLICY DATA STORE
220
ENABLE SECURITY MODE A
300
ENABLE SECURITY MODE B
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
VISUAL INDICATION
350
VISUAL INDICATION
250
USER
352
USER

FIG. 5

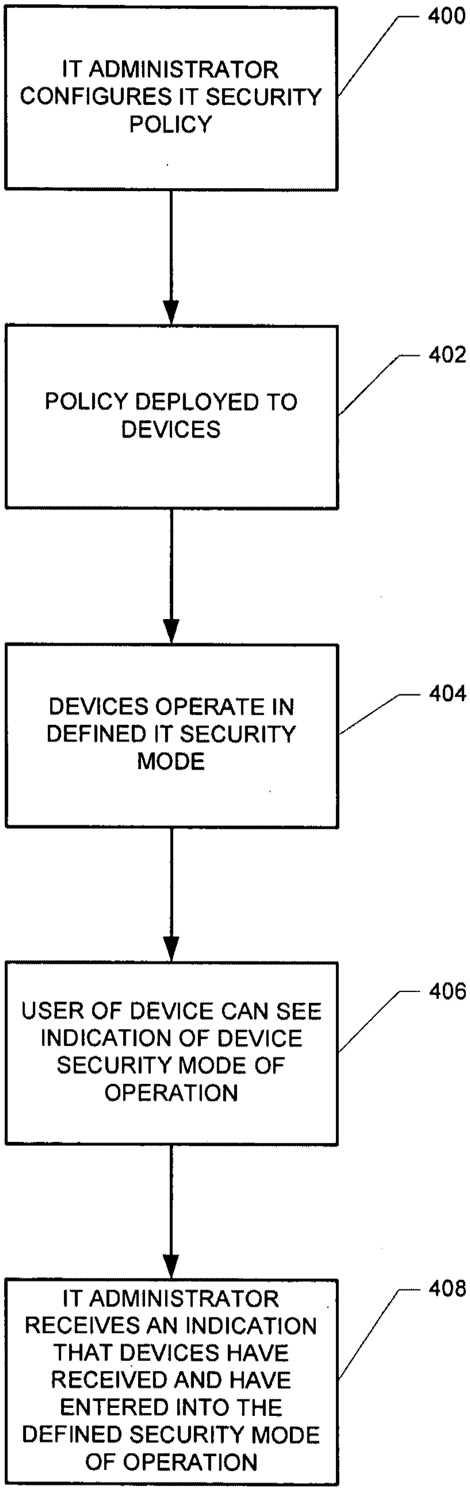

IT ADMINISTRATOR CONFIGURES IT SECURITY POLICY
400
POLICY DEPLOYED TO DEVICES
402
DEVICES OPERATE IN DEFINED IT SECURITY MODE
404
USER OF DEVICE CAN SEE INDICATION OF DEVICE SECURITY MODE OF OPERATION
406
IT ADMINISTRATOR RECEIVES AN INDICATION THAT DEVICES HAVE RECEIVED AND HAVE ENTERED INTO THE DEFINED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

FIG. 6

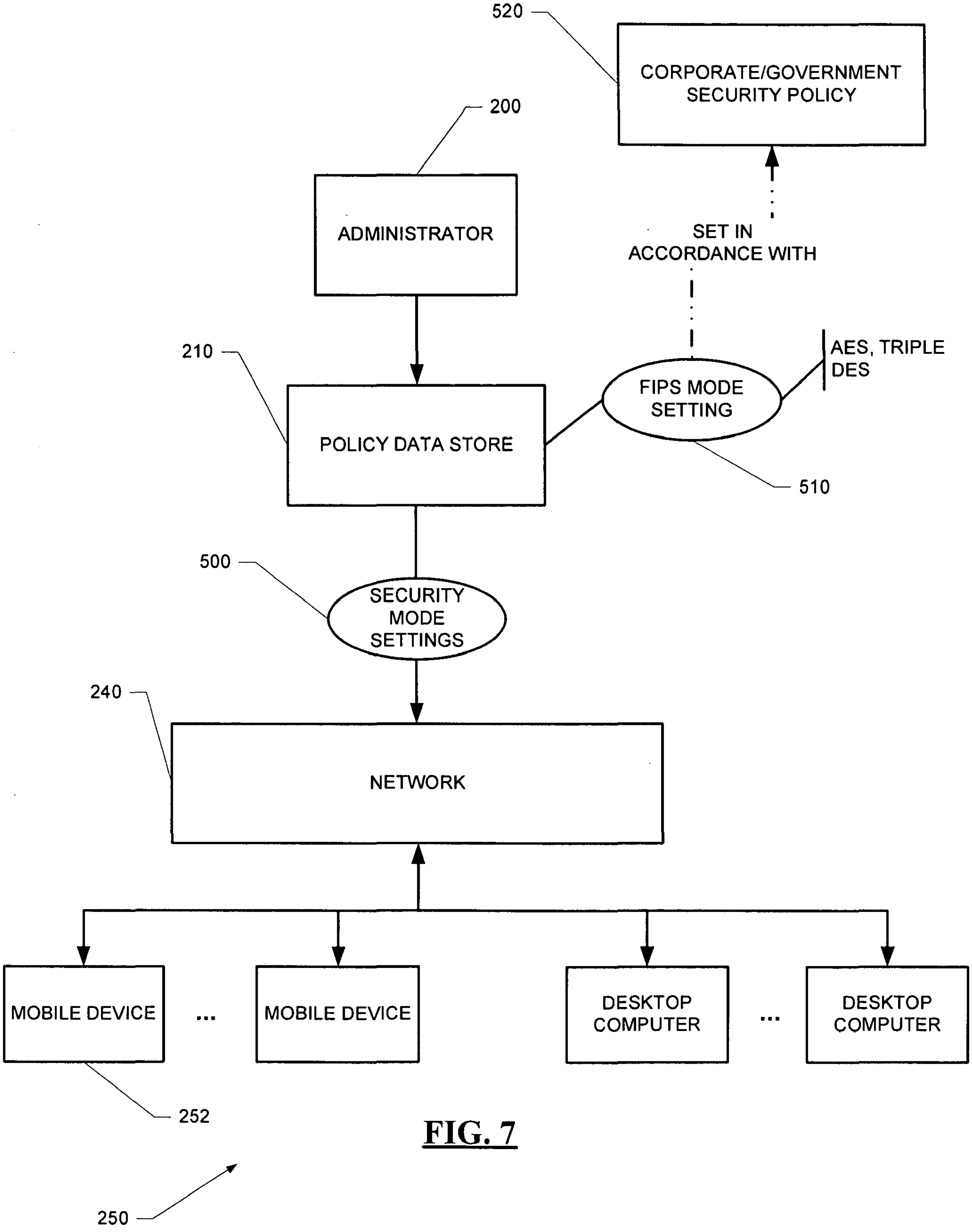

520
CORPORATE/GOVERNMENT SECURITY POLICY
200
ADMINISTRATOR
SET IN ACCORDANCE WITH
210
POLICY DATA STORE
FIPS MODE SETTING
AES, TRIPLE DES
510
500
SECURITY MODE SETTINGS
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP COMPUTER
252
250

FIG. 7

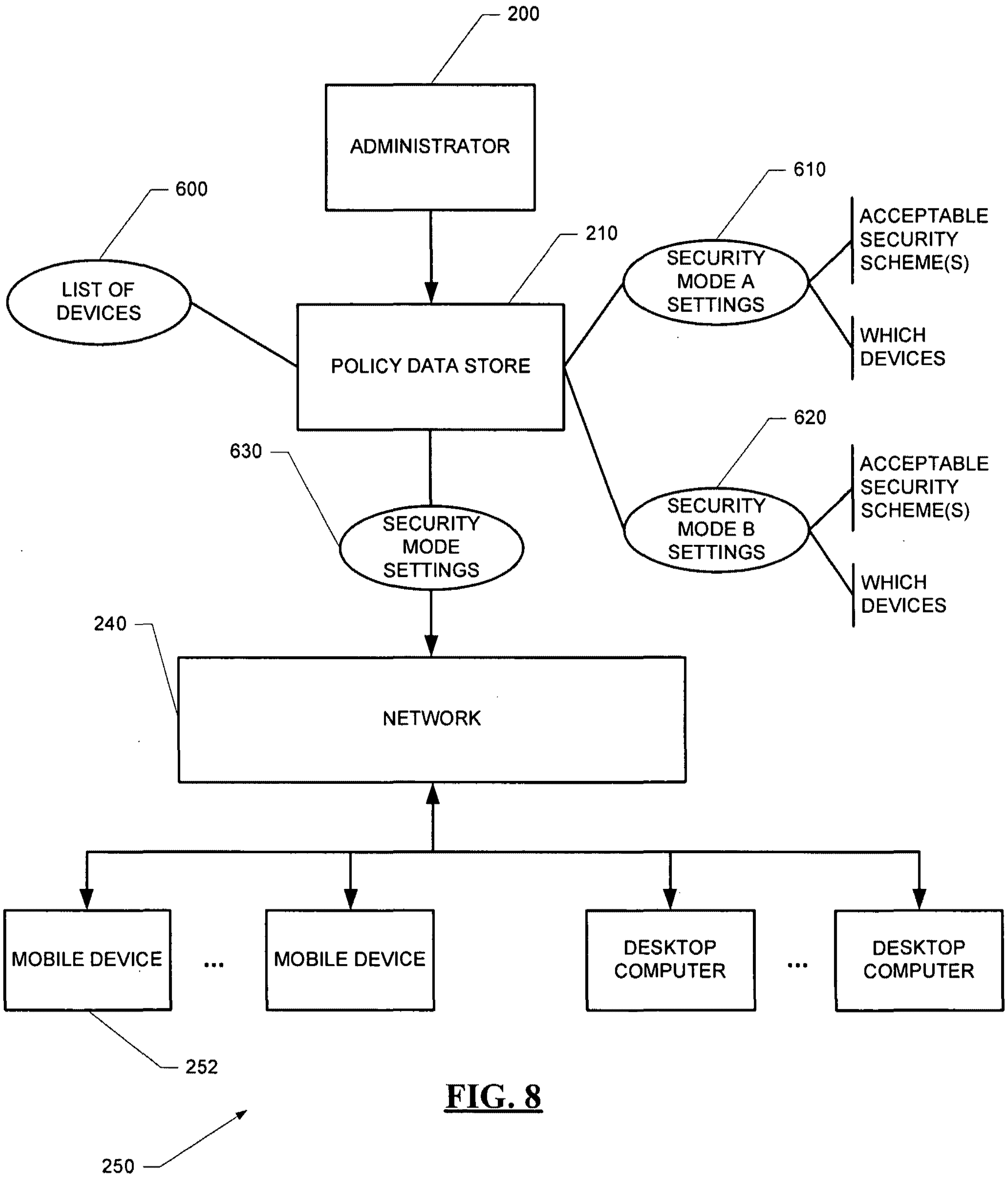

200
ADMINISTRATOR
600
LIST OF DEVICES
210
POLICY DATA STORE
610
SECURITY MODE A SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
620
SECURITY MODE B SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
630
SECURITY MODE SETTINGS
240
NETWORK
MOBILE DEVICE
...
MOBILE DEVICE
DESKTOP COMPUTER
...
DESKTOP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

FIG. 8

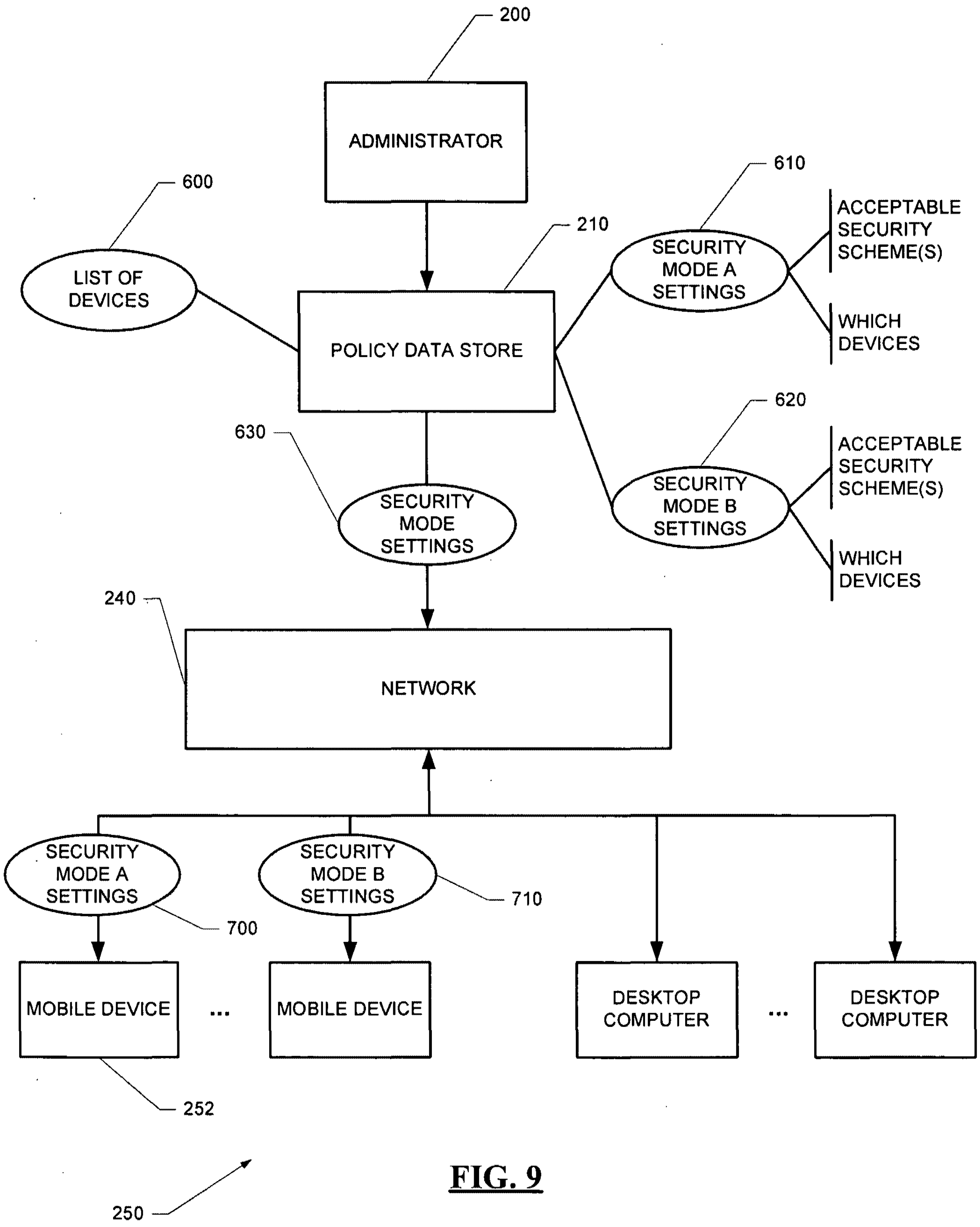

200
ADMINISTRATOR
600
LIST OF DEVICES
210
POLICY DATA STORE
610
SECURITY MODE A SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
620
SECURITY MODE B SETTINGS
ACCEPTABLE SECURITY SCHEME(S)
WHICH DEVICES
630
SECURITY MODE SETTINGS
240
NETWORK
SECURITY MODE A SETTINGS
700
SECURITY MODE B SETTINGS
710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

FIG. 9

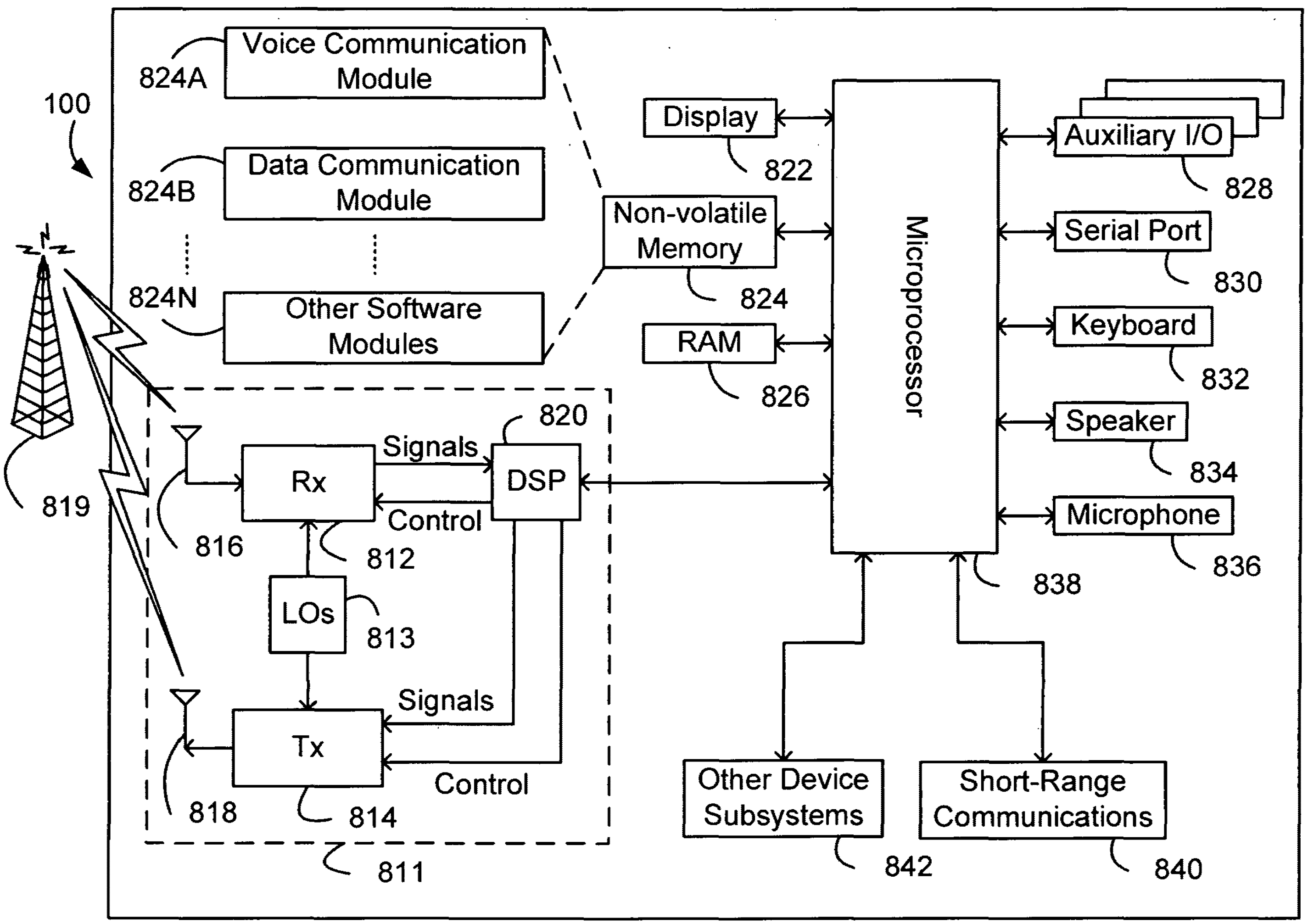

100
824A
Voice Communication Module
824B
Data Communication Module
824N
Other Software Modules
Display
822
Non-volatile Memory
824
RAM
826
Microprocessor
Auxiliary I/O
828
Serial Port
830
Keyboard
832
Speaker
834
Microphone
836
838
819
820
Signals
DSP
Rx
Control
816
812
LOs
813
Signals
Tx
Control
818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

FIG. 10

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	ATTORNEY DOCKET NUMBER
11/065,901	02/25/2005	Neil P. Adams	555255-012798

CONFIRMATION NO. 4175

FORMALITIES LETTER

OC000000016174820

John V. Biernacki, Esq.
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Date Mailed: 06/02/2005

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.* *Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.*
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a Large Entity

- **$130** Late oath or declaration Surcharge.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

Office of Initial Patent Examination (703) 308-1202

PART 3 - OFFICE COPY

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	ATTORNEY DOCKET NUMBER
11/065,901	02/25/2005	Neil P. Adams	555255-012798

CONFIRMATION NO. 4175

FORMALITIES LETTER

OC000000016174820

John V. Biernacki, Esq.
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Date Mailed: 06/02/2005

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a Large Entity

- **$130** Late oath or declaration Surcharge.

Replies should be mailed to:
Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice <u>MUST</u> be returned with the reply.

Office of Initial Patent Examination (703) 308-1202

PART 2 - COPY TO BE RETURNED WITH RESPONSE

PATENT

Attorney Docket No. 555255012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Neil P. Adams, et al.
Serial No.:	11/065,901
Filed:	February 25, 2005
For:	SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS
Art Unit:	Not yet assigned
Examiner:	Not yet assigned

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

In response to the Notice to File Missing Parts of Nonprovisional Application, Filing Date Granted, mailed June 2, 2005, a copy of which is returned herewith, enclosed are the following papers relating to the above-identified application:

- Declaration (4 pages),
- Power of Attorney (1 page),
- Statement Under 37 CFR 3.73(b) (1 page),
- Copy of Assignment (8 pages).

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on July 26, 2005
By: Jacquie Ofner

The Commissioner is hereby authorized to charge the late filing fee/surcharge of $130, and any additional fees necessary with this response, or to credit any overpayment, to Jones Day's Deposit Account, No. 501432 (ref. 555255012798). A copy of this Response is enclosed for processing the charge to the Deposit Account.

Respectfully submitted,

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939

Date: July 26, 2005

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
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 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 22 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 22 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))	Family Name or Surname			
Michael S.	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))	Family Name or Surname			
Michael G.	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))	Family Name or Surname			
Herbert A.	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 22 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 22 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.

PTO/SB/80 (12-03)
Approved for use through 11/30/2005. 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 appoint:

☑ Practitioners associated with the Customer Number: 24325

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

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).

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

Name	Mihal Lazaridis		
Signature		Date	JAN 16, 2004
Title	President & Co-CEO	Telephone	519-888-7465

This collection of information is required by 37 CFR 1.31 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 1.14. 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 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Neil P. Adams, et al. / Research In Motion Limited

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

Entitled: 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; or

2. □ an assignee of less than the entire right, title and interest.
The extent (by percentage) of its ownership interest is ______%
in 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 ________, Frame ________, or for which a copy thereof is attached.

OR

B. [ ] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

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.

[ ] Copies of assignments or other documents in the chain of title are attached.
[NOTE: A separate copy (*i.e.*, the original assignment document or a true copy of the original document) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded 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.

July 26, 2005
Date

John V. Biernacki Regn. No. 40,511
Typed or printed name

216-586-3939
Telephone number

John Biernacki
Signature

Attorney (Agent) for Assignee
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 1.14. 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.

IFW

PATENT

Attorney Docket No. 555255012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Neil P. Adams, et al.
Serial No.:	11/065,901
Filing Date:	February 25, 2005
For:	SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS
Art Unit:	Not yet assigned
Examiner:	Not yet assigned

Mail Stop Amendment
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure imposed by 37 C.F.R. § 1.56, applicants hereby advise the United States Patent and Trademark Office of certain references which may be material to the determination of patentability of the above-identified application. The references are identified on the attached Form PTO-1449; copies are enclosed, if required. Applicants respectfully request that these references be considered and made of record in the present application by completing and returning the enclosed Form PTO-1449.

No fee is believed to be due for entry of this Information Disclosure Statement. However, if any fee should be required, please charge such fee to Jones Day's Deposit Account No. 501432, Reference No. 555255012798.

Respectfully submitted,

John V. Biernacki Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on March 24, 2006
By:

March 24, 2006

Page 1 of 1

CLI-1397136v1

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. 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 contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

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

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 6202157 B1	03-13-2001	Brownlie, et al.	
		US- 6732168 B1	05-04-2004	Bearden, et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 0069120 A1	11-16-2000			☐
						☐
						☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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/08B (08-03)
Approved for use through 07/31/2006. 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 contains a valid OMB control number.

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application Number**	11/065,901
				Filing Date	February 25, 2005
				First Named Inventor	Neil P. Adams
(Use as many sheets as necessary)				Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	2	of	2	Attorney Docket Number	555255-012798

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		International Search Report of Application No. PCT/CA2005/000294, date of mailing June 20, 2005 - 11 pgs	

Examiner Signature		Date Considered	

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

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 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 2 hours 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, 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.

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.

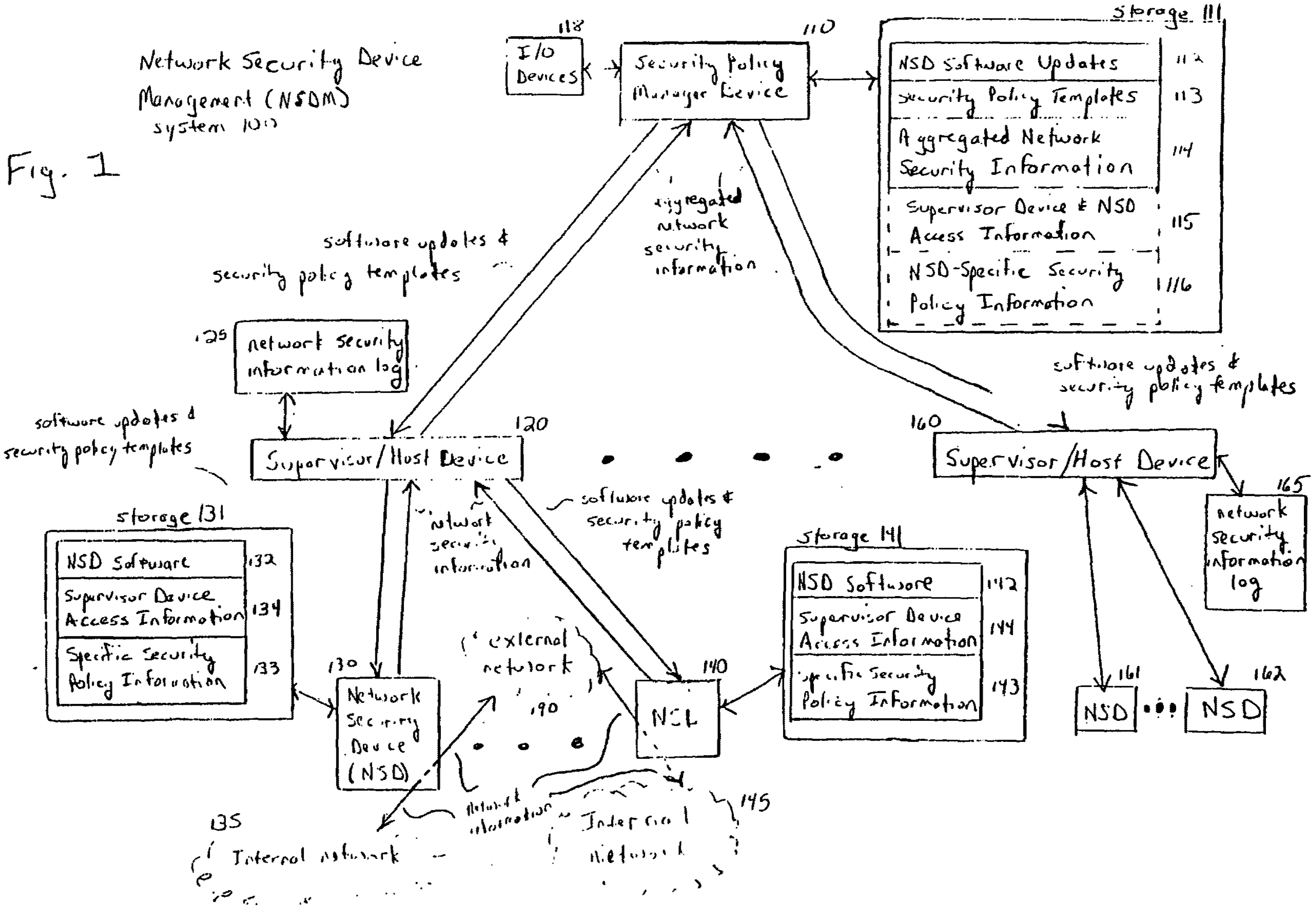
103. The data signal of claim 102 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

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.

Fig. 1

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
125
network security information log
software updates & security policy templates
120
Supervisor/Host Device
160
Supervisor/Host Device
software updates & security policy templates
165
network security information log
storage 131
NSD Software
132
Supervisor Device Access Information
134
Specific Security Policy Information
133
network security information
software updates & security policy templates
storage 141
NSD Software
142
Supervisor Device Access Information
144
Specific Security Policy Information
143
130
Network Security Device (NSD)
external network
190
140
NSD
161
NSD
162
NSD
135
Internal network
network information
Internal network
145

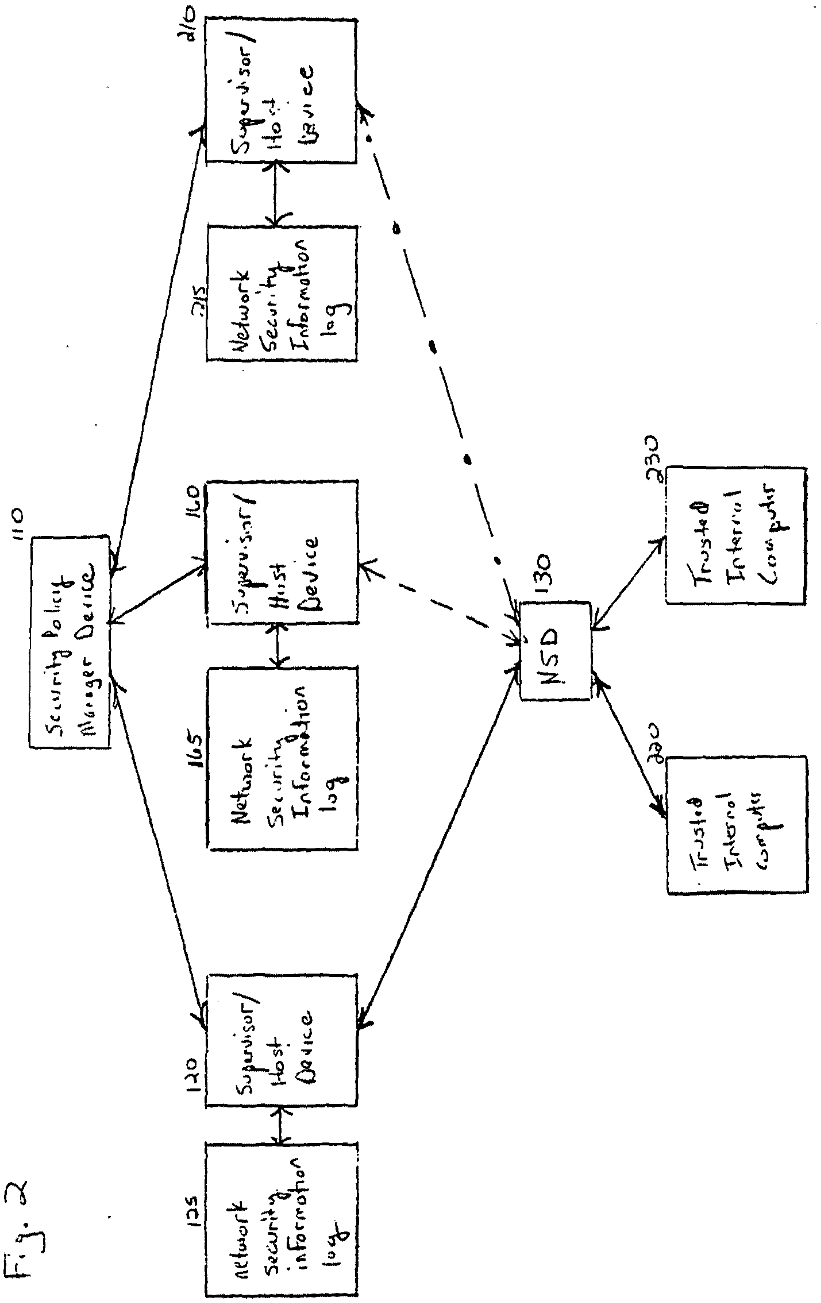

110
Security Policy Manager Device
120
Supervisor/Host Device
125
Network Security information log
160
Supervisor/Host Device
165
Network Security Information log
210
Supervisor/Host Device
215
Network Security Information log
130
NSD
220
Trusted Internal Computer
230
Trusted Internal Computer

Fig. 2

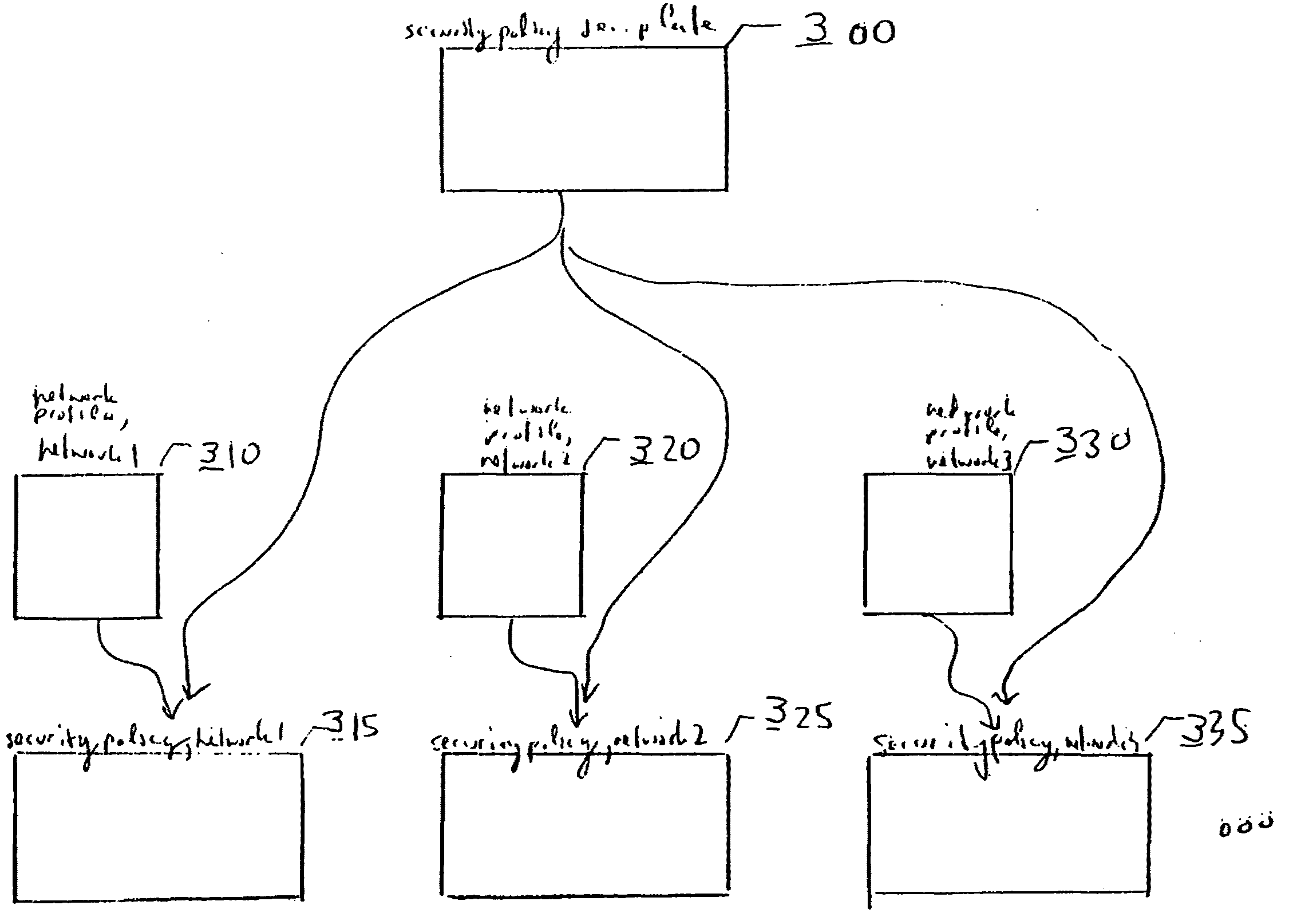

security policy template
300
network profile, network 1
310
network profile, network 2
320
network profile, network 3
330
security policy, network 1
315
security policy, network 2
325
security policy, network 3
335
ooo

Fig. 3A

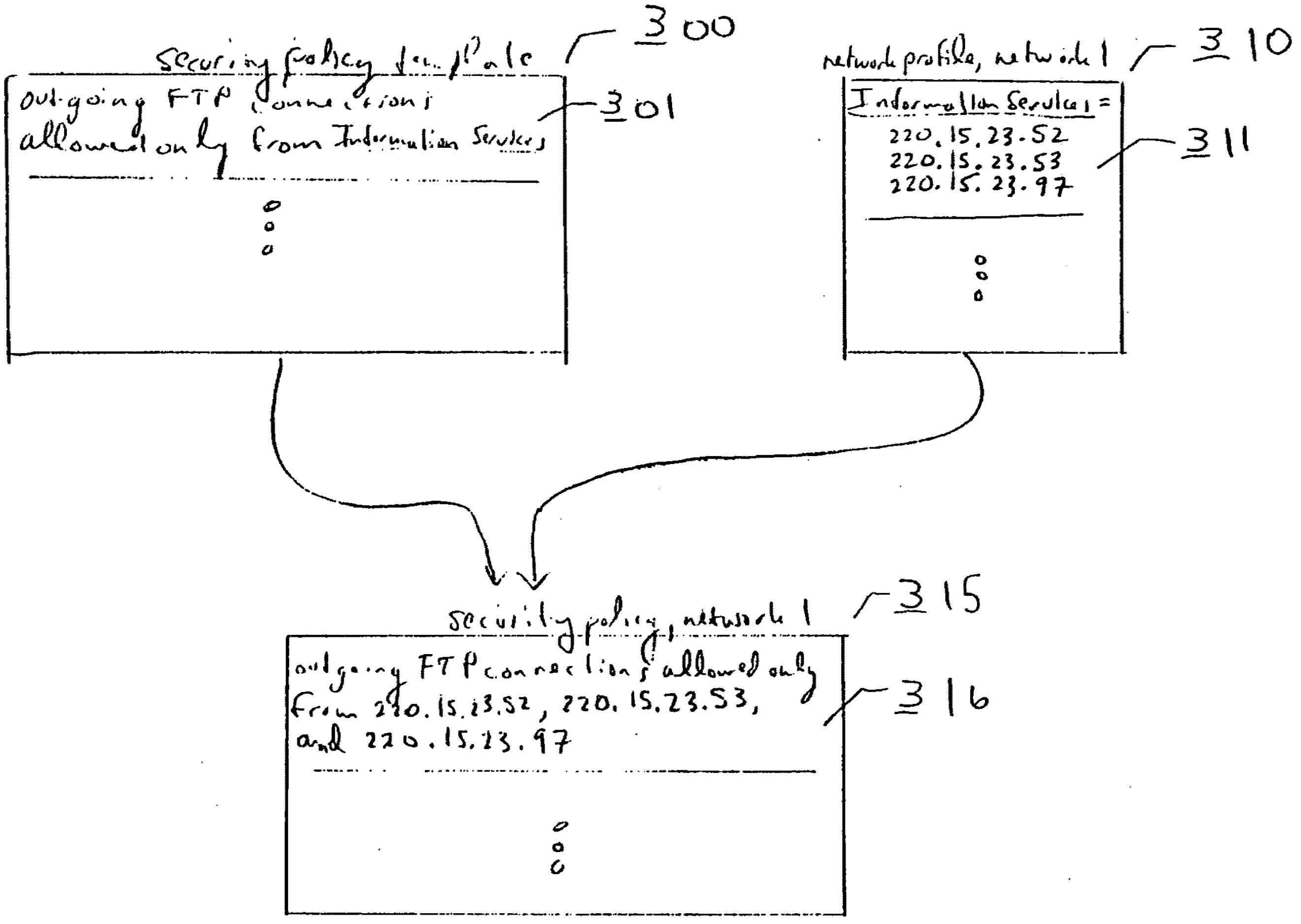
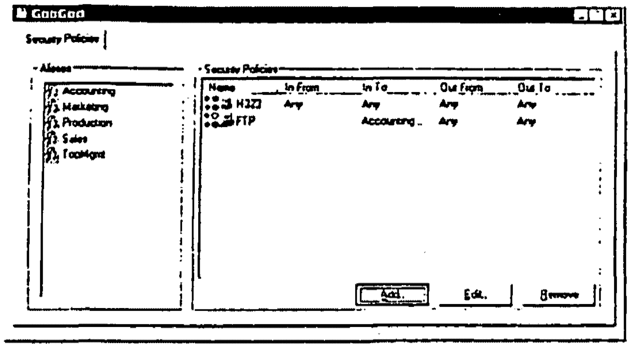

security policy template
300
outgoing FTP connections allowed only from Information Services
301
network profile, network 1
310
Information Services =
220.15.23.52
220.15.23.53
220.15.23.97
311
security policy, network 1
315
outgoing FTP connections allowed only from 220.15.23.52, 220.15.23.53, and 220.15.23.97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

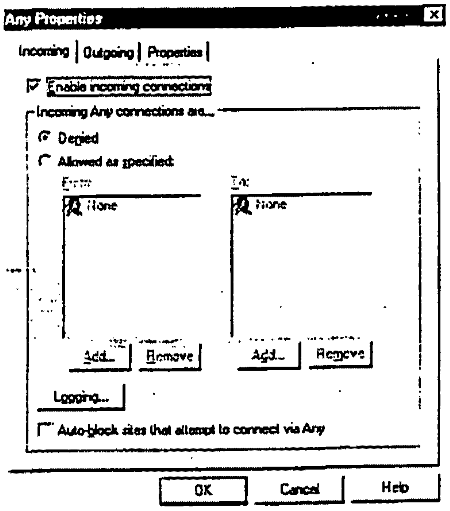
Fig. 3B



Aliases:
- Accounting
- Marketing
- Production
- Sales
- ToolMgmt

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

Fig. 3C



☑ Enable incoming connections

Incoming Any connections are...

● Denied

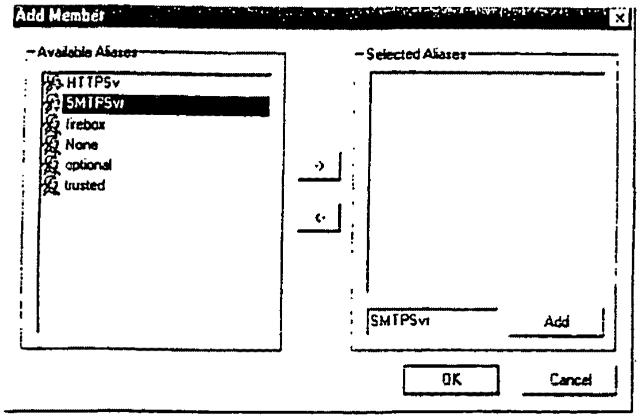
○ Allowed as specified

From: None

To: None

□ Auto-block sites that attempt to connect via Any

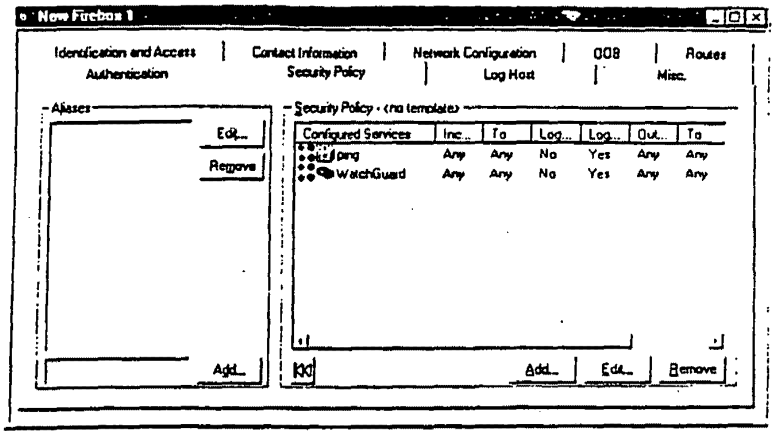
Fig. 3D



Available Aliases:
- HTTPSvr
- SMTPSvr
- firebox
- None
- optional
- trusted

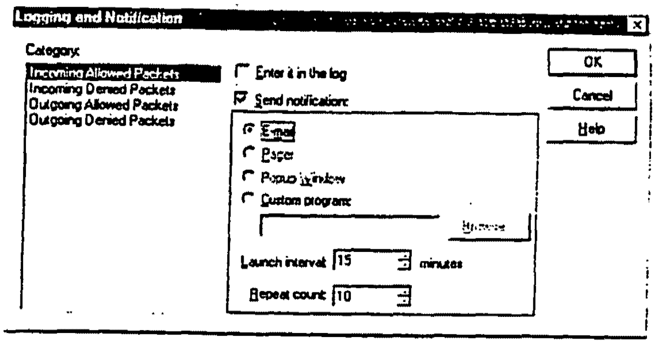
SMTPSvr

Fig. 3E


New Firebox 1

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

Fig. 3F


Logging and Notification

Category:

- Incoming Allowed Packets
- Incoming Denied Packets
- Outgoing Allowed Packets
- Outgoing Denied Packets

□ Enter it in the log

☑ Send notification:

● E-mail

○ Pager

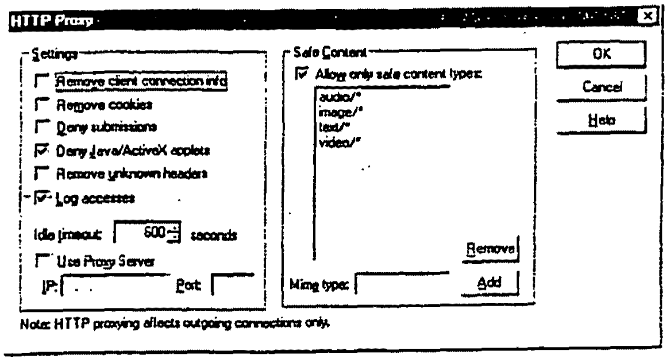
○ Popup window

○ Custom program:

Launch interval: 15 minutes

Repeat count: 10

Fig. 3G


HTTP Proxy

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)
```

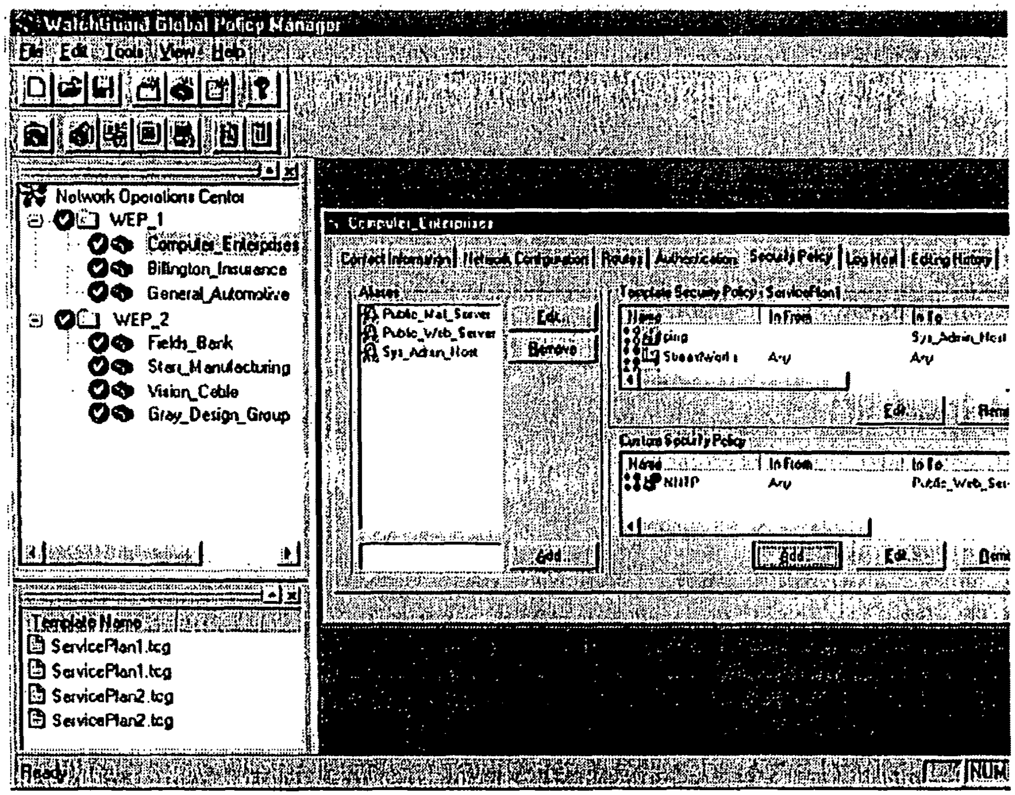
Fig. 4F

```
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



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

Public_Mail_Server
Public_Web_Server
Sys_Admin_Host

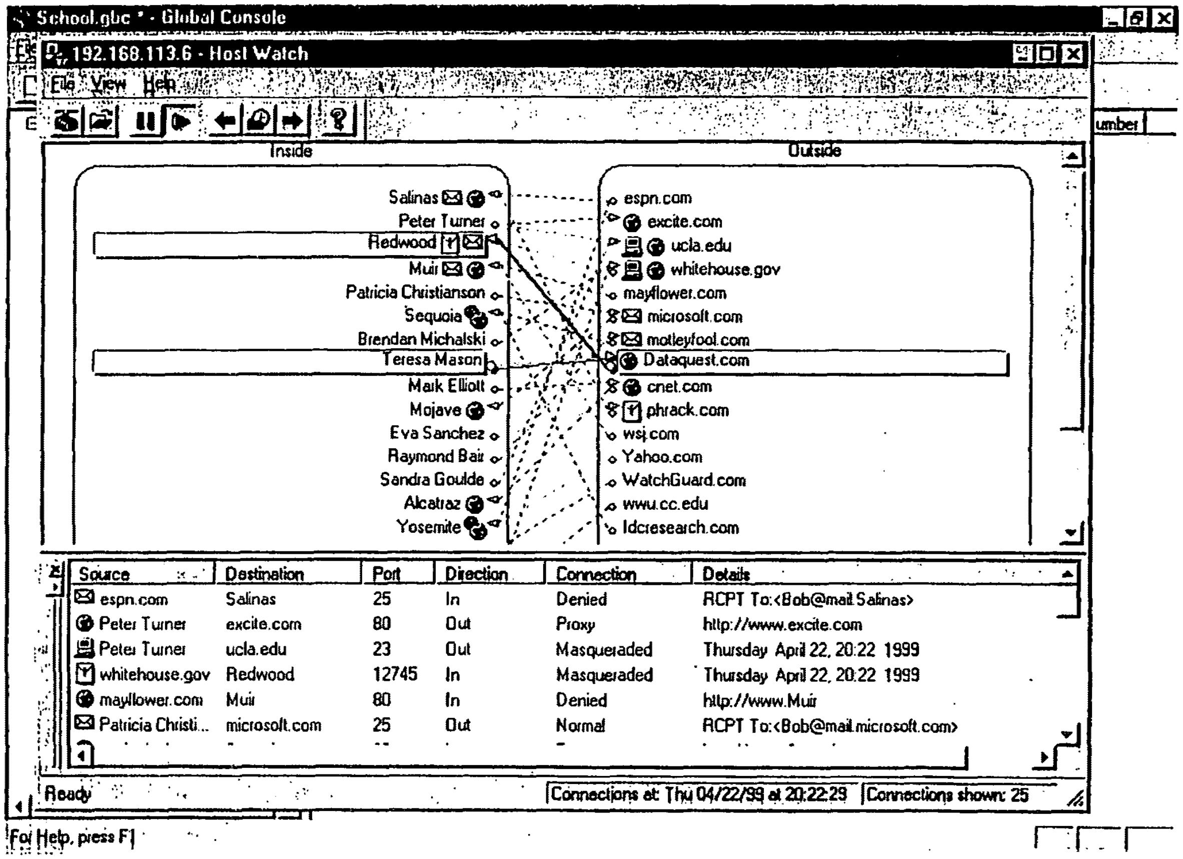
Template Security Policy: ServicePlan1

Name	In From	In To
ping		Sys_Admin_Host
SmartWorks	Any	Any

Custom Security Policy

Name	In From	In To
NNTP	Any	Public_Web_Ser

Fig. 5A

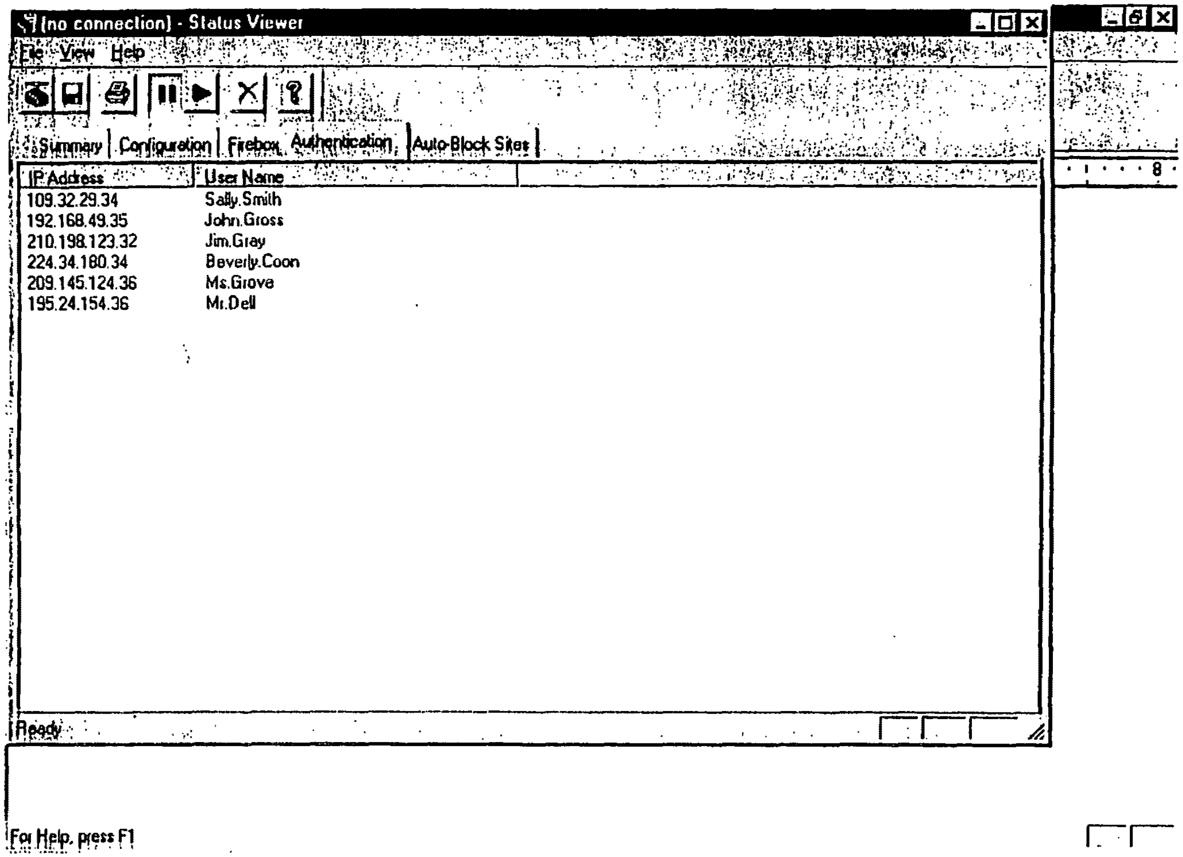


Source	Destination	Port	Direction	Connection	Details
☒ espn.com	Salinas	25	In	Denied	RCPT To:<Bob@mail.Salinas>
● Peter Turner	excite.com	80	Out	Proxy	http://www.excite.com
Peter Turner	ucla.edu	23	Out	Masqueraded	Thursday April 22, 20:22 1999
whitehouse.gov	Redwood	12745	In	Masqueraded	Thursday April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

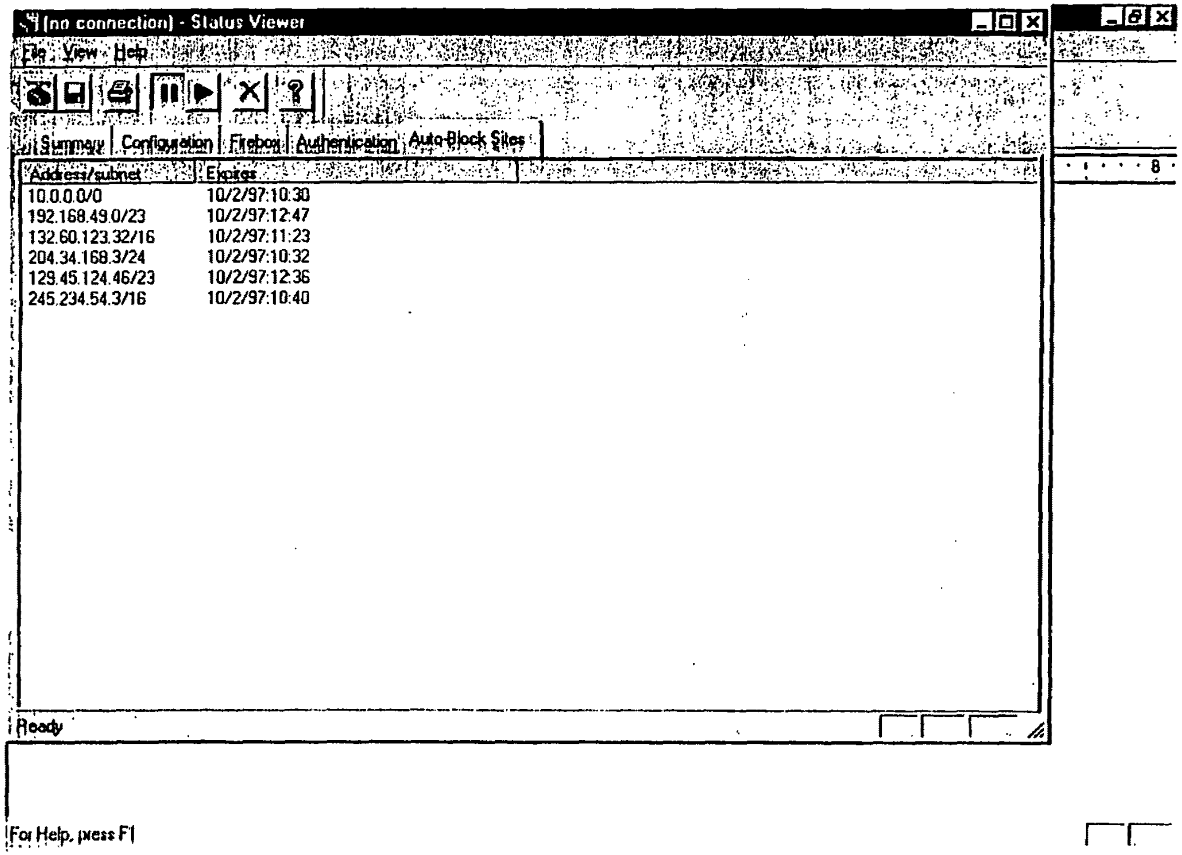
For Help, press F1

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.Grova
195.24.154.36	Mr.Dell

Fig. 5C

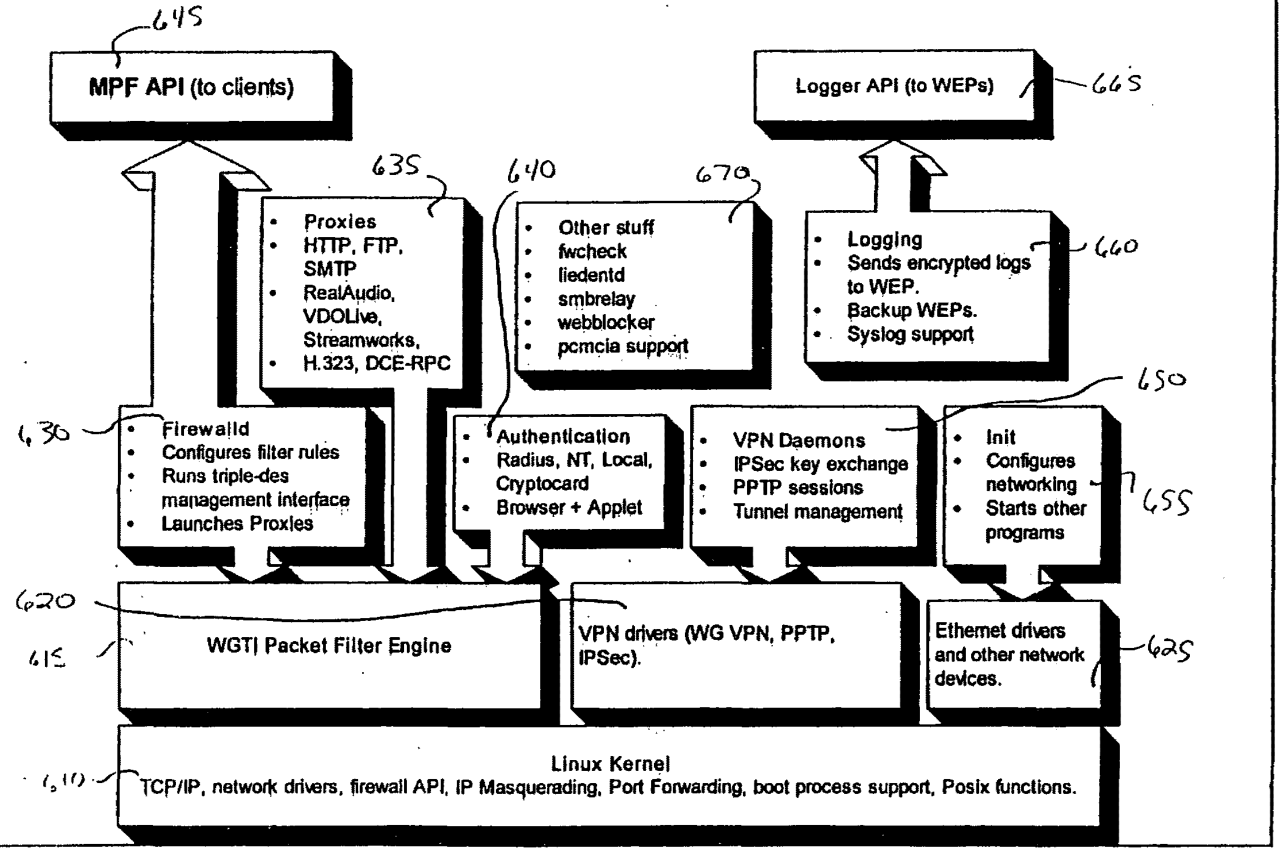


Address/subnet	Expires
10.0.0.0/0	10/2/97:10:30
192.168.49.0/23	10/2/97:12:47
132.60.123.32/16	10/2/97:11:23
204.34.168.3/24	10/2/97:10:32
129.45.124.46/23	10/2/97:12:36
245.234.54.3/16	10/2/97:10:40

Fig. 5D.

Fig. 6

Appliance Architecture



MPF API (to clients)

Logger API (to WEPs)

- 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.

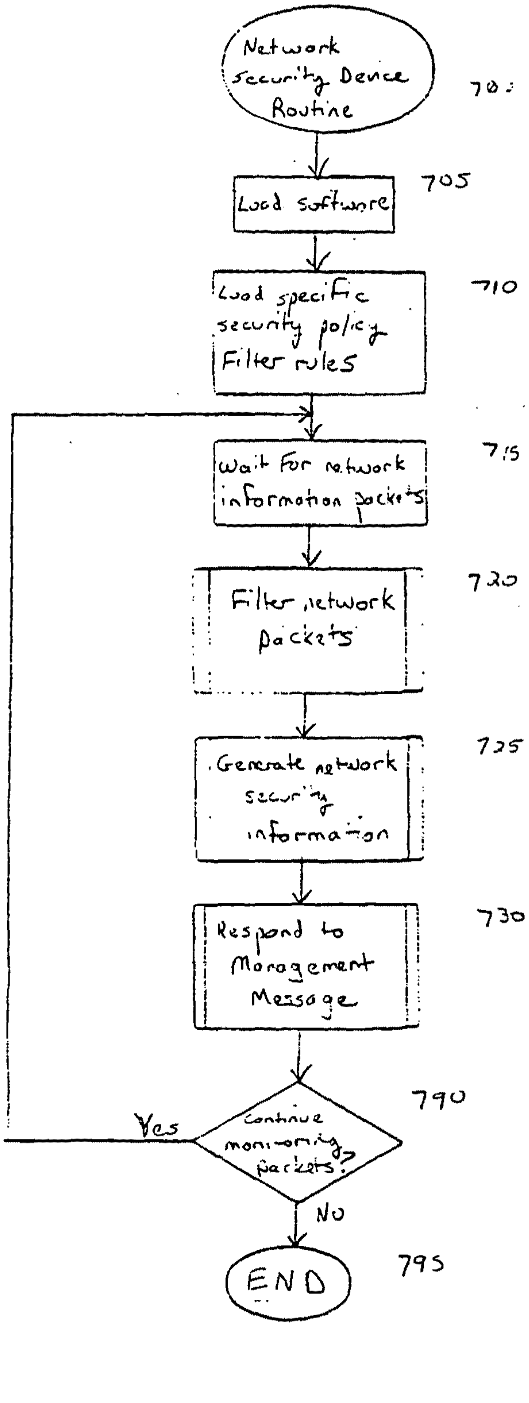

Network Security Device Routine
70:
Load software
705
Load specific security policy Filter rules
710
Wait for network information packets
715
Filter network packets
720
Generate network security information
725
Respond to Management Message
730
continue monitoring packets?
790
Yes
No
END
795

Fig. 7

Fig. 8

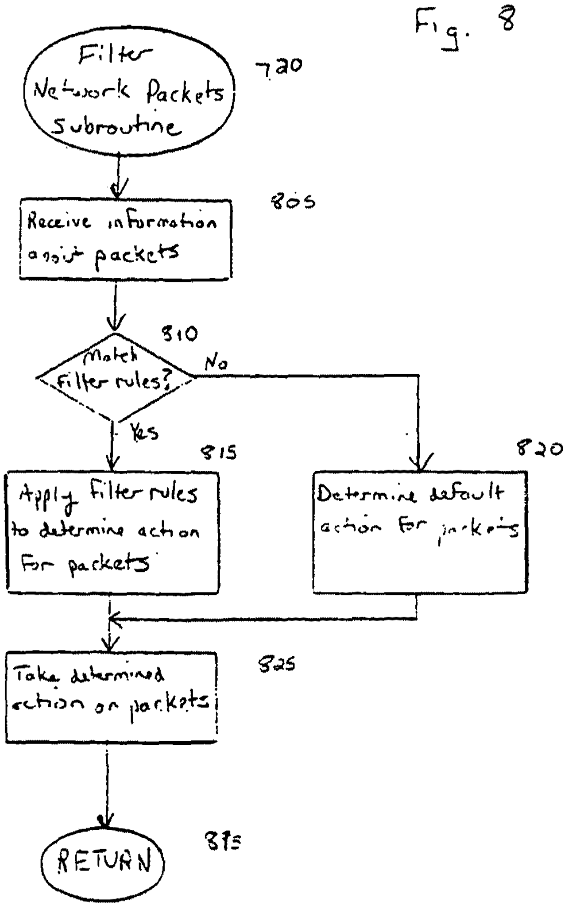
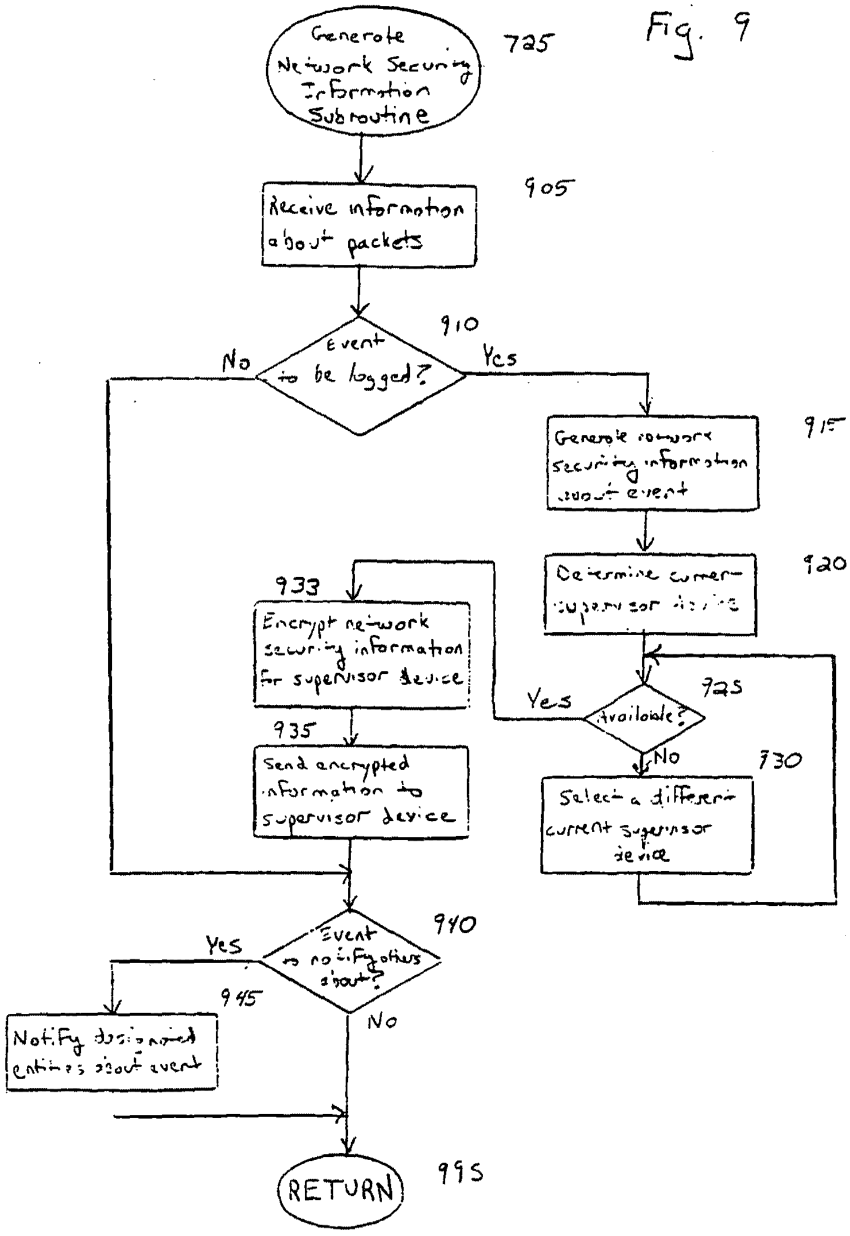

Filter Network Packets Subroutine
720
Receive information about packets
805
Match Filter rules?
810
No
Yes
Apply Filter rules to determine action for packets
815
Determine default action for packets
820
Take determined action on packets
825
RETURN
815

Fig. 9


Generate Network Securing Information Subroutine
725
Receive information about packets
905
Event to be logged?
910
No
Yes
Generate network securing information about event
915
Determine current supervisor device
920
Available?
725
Yes
No
Select a different current supervisor device
730
Encrypt network securing 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

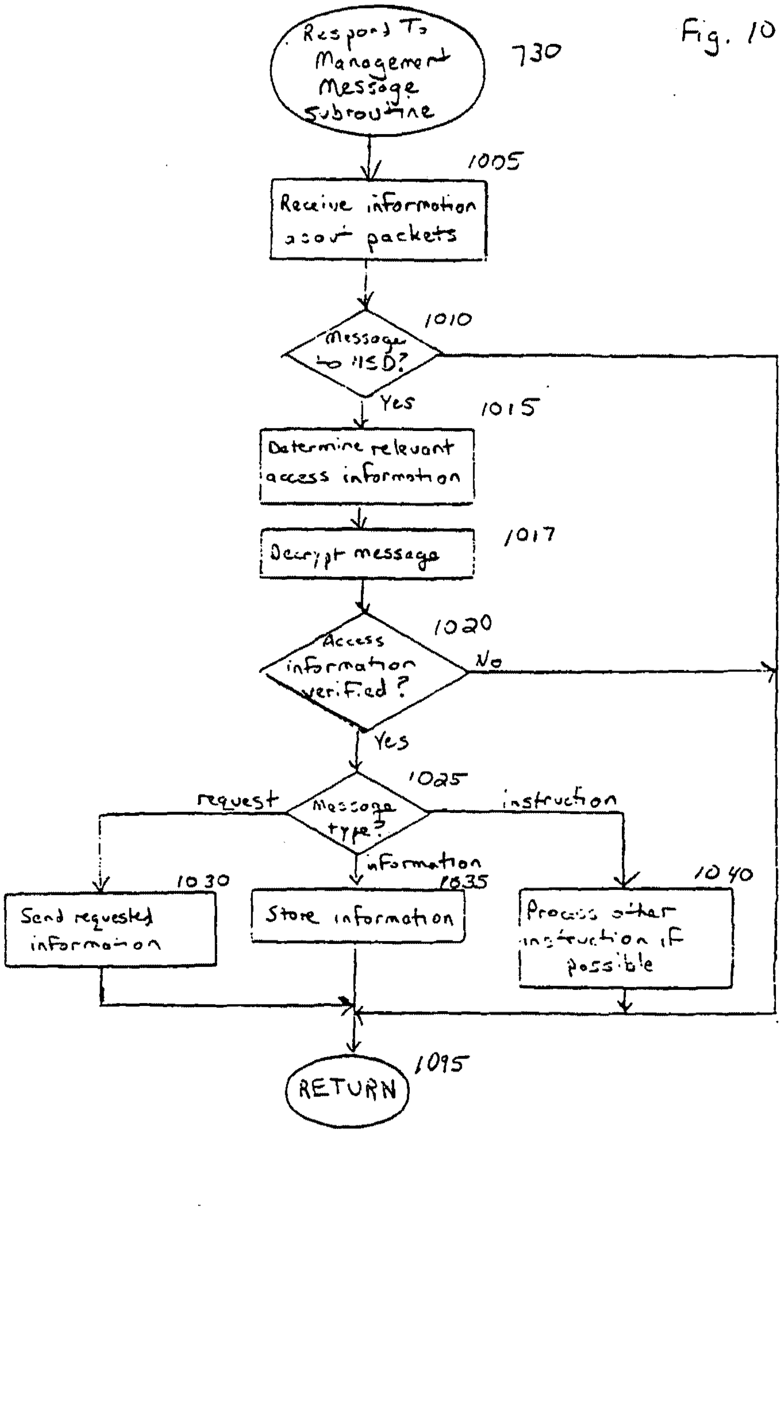

Respond To Management Message Subroutine
730
1005
Receive information about packets
1010
Message to HSD?
Yes
1015
Determine relevant access information
1017
Decrypt message
1020
Access information verified?
No
Yes
1025
Message type?
request
instruction
information
1030
1035
1040
Send requested information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

Fig. 10

Fig. 11

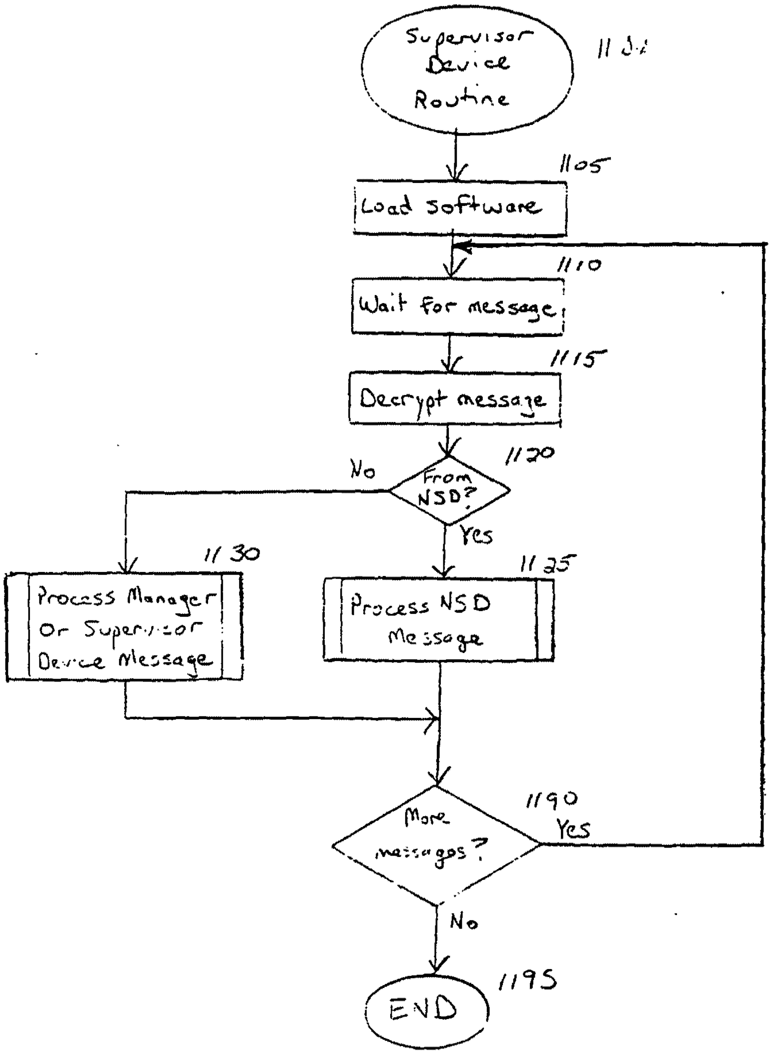
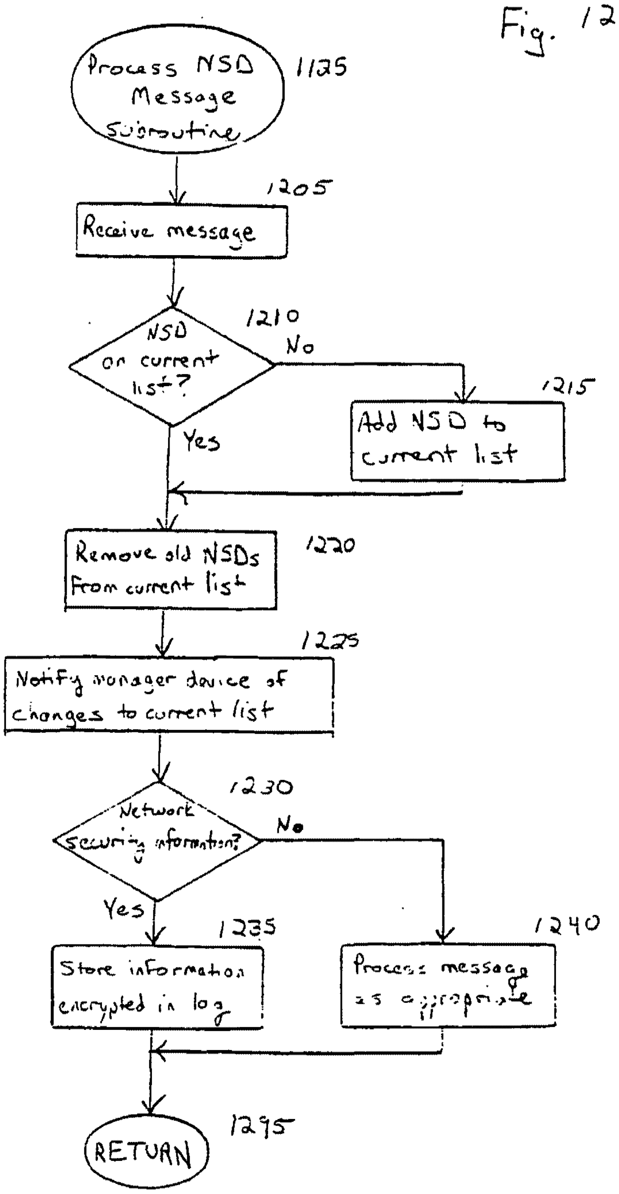

Supervisor Device Routine
1100
Load software
1105
Wait for message
1110
Decrypt message
1115
From NSD?
1120
No
Yes
Process Manager Or Supervisor Device Message
1130
Process NSD Message
1125
More messages?
1190
Yes
No
END
1195

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 securing information?
No
Yes
1235
1240
Store information encrypted in log
Process message as appropriate
1295
RETURN

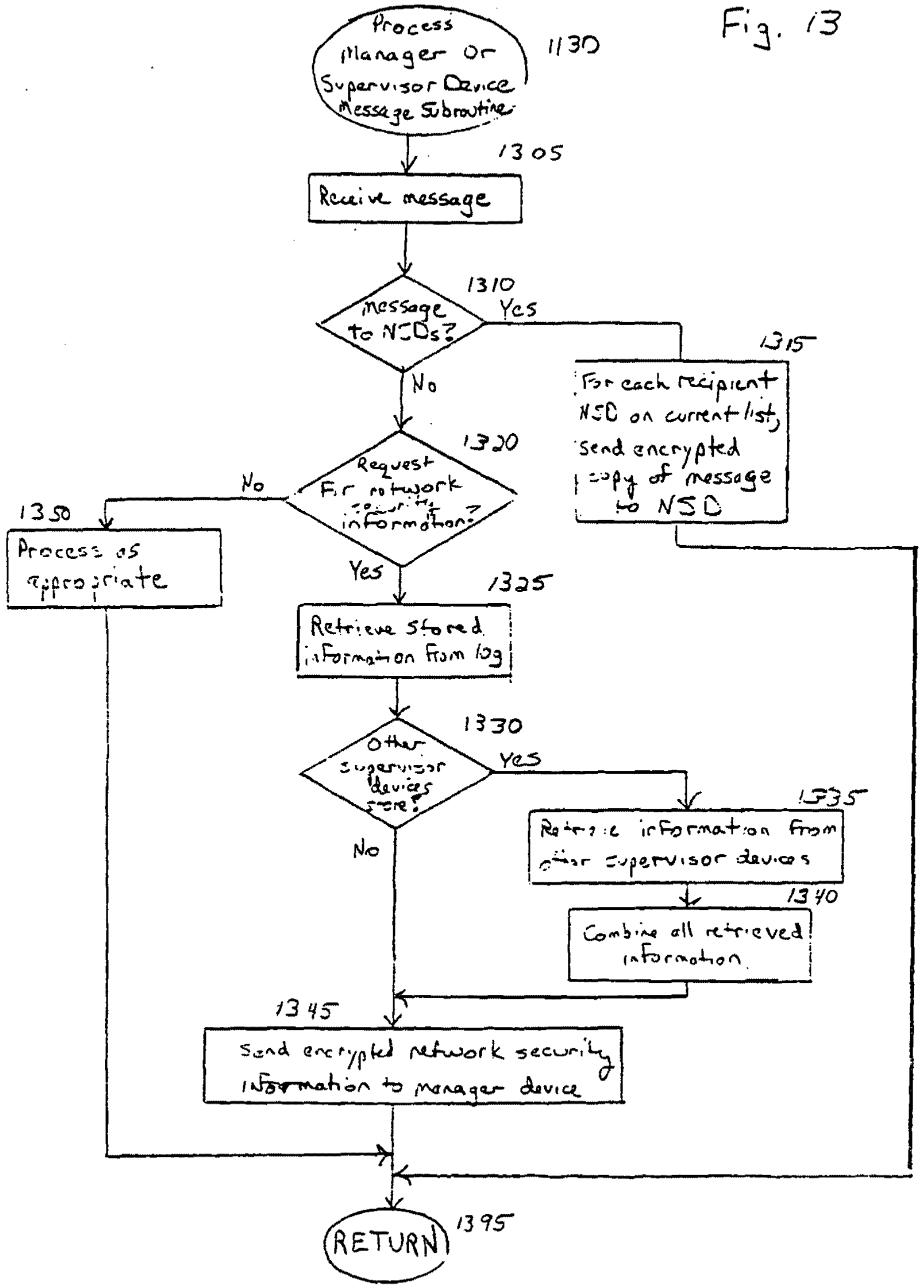

Process Manager Or Supervisor Device Message Subroutine
1130
1305
Receive message
1310
message to NSDs?
Yes
No
1315
For each recipient NSD on current list, send encrypted copy of message to NSD
1320
Request For network security information?
No
Yes
1350
Process as appropriate
1325
Retrieve stored information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

Fig. 13

Fig. 14A

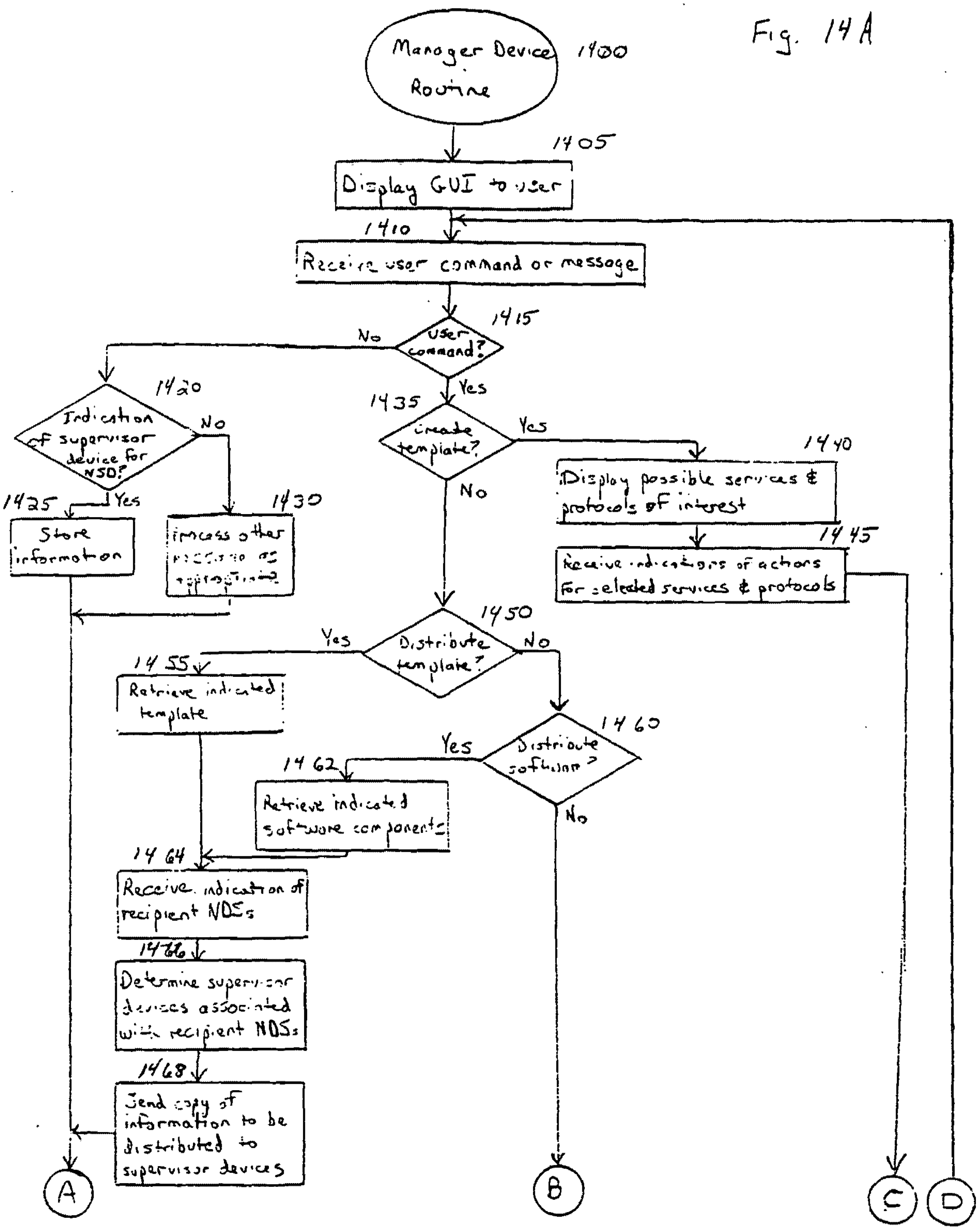
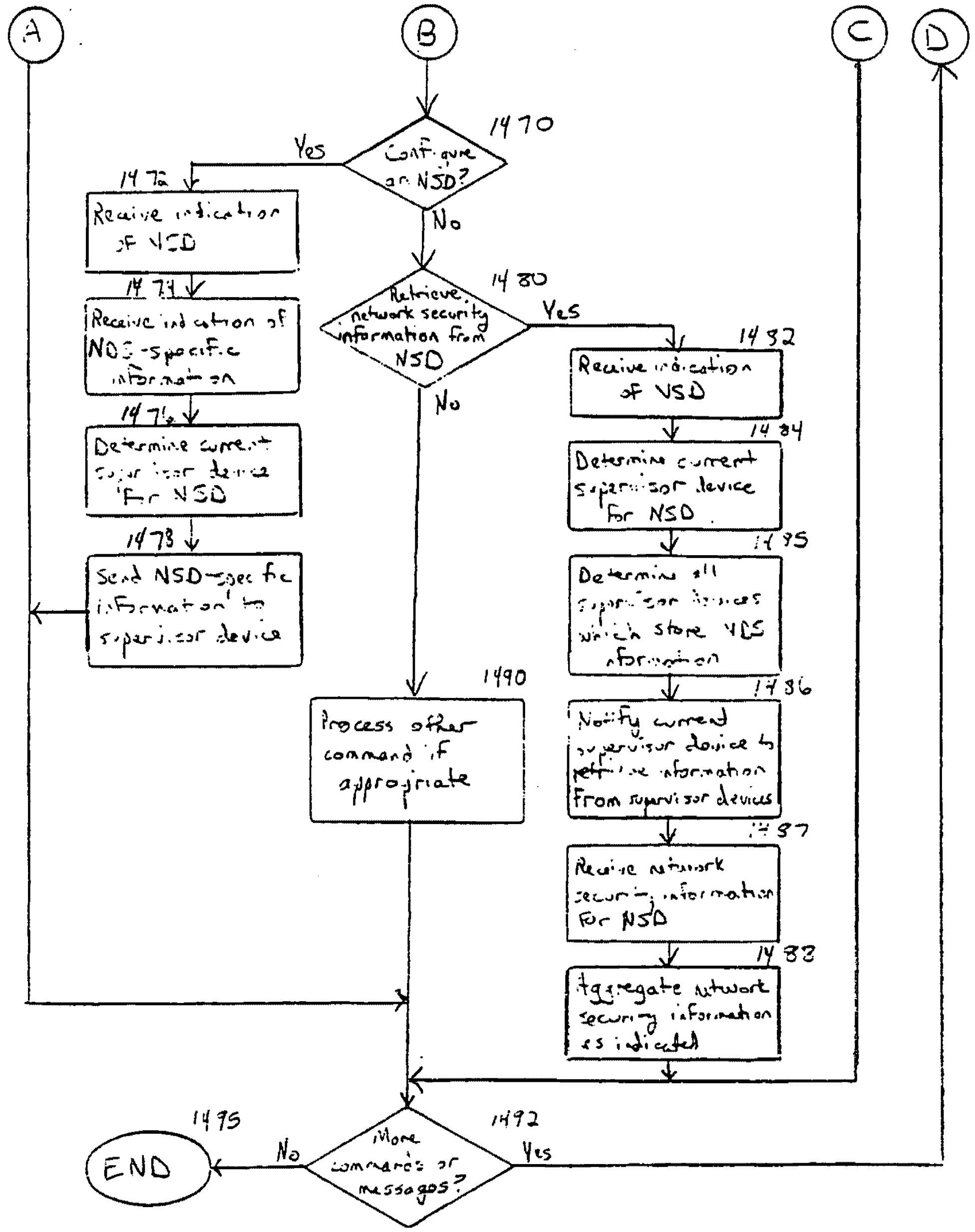

Manager Device Routine
1400
1405
Display GUI to user
1410
Receive user command or message
1415
User command?
No
Yes
1420
Indication of supervisor device for NSD?
No
Yes
1425
Store information
1430
Process other messages as appropriate
1435
Create template?
Yes
No
1440
Display possible services & protocols 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 NSD-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

1

INTERNATIONAL SEARCH REPORT

Inten 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

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

7590 02/06/2008

John V. Biernacki, Esq.
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
4158	

MAIL DATE	DELIVERY MODE
02/06/2008	PAPER

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.

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 11/065,901	**Applicant(s)** ADAMS ET AL.	
	Examiner BRYAN F. WRIGHT	**Art Unit** 4158	

-- 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 *25 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☒ Claim(s) *6 and 12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *2/25/2005* 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).

11)☐ 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

12)☐ 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 *3/27/2006*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of February 25, 2005. Claims (1-22) are pending and have been considered below.

Drawings

2. The drawings are objected to because fig. 1, reference items 15, 25, and 95 are missing identification labels. Also, fig. 2, reference items 15, 25, 50, 80, and 100 are missing identification labels. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

Claim Objections

4. Claims 6 and 12 are objected to because of the following informalities: The usage of the term "*uses*" renders the claim indefinite and does not clearly and concisely limit the bounds of the clams. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. Regarding claim 22, the word "means" is preceded by the word(s) for receiving, for entering, and for displaying in an attempt to use a "means" clause to recite a claim

element as a means for performing a specified function. However, since no function is specified by the word(s) preceding "means," it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph. See *Ex parte Klumb*, 159 USPQ 694 (Bd. App. 1967).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 4-18, and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Schoen et al. (US Patent Publication No. 2003/0204722 and Schoen hereinafter).

8. As to claims 1, 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 security mode data structure stores a security mode of operation (par. 69, line 13-15);

where the stored security mode of operation is provided to the computing devices over a network (par. 73, lines 16-20);

where the security mode of operation places the computing devices in a predetermined security mode of operation (par. 69, line 13-15);

where the 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 (par. 65, lines 17-21).

9. 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).

10. 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).

11. 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).

12. As to claim 7, 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).

13. As to claim 8, Schoen discloses 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 (par. 69, lines 21-32);

and a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (Schoen; claim 10, lines 2-5);

where 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 (Schoen: claim 9, lines 4-7).

14. As to claim 9, Schoen discloses a device where 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 (par. 65, lines 17-21).

15. As to claim 10, Schoen discloses a system where the visual indication of the security mode is provided by a security options screen (par. 65, lines 17-21).

16. As to claim 11, Schoen discloses a device where the 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. 30, lines 3-7), where a visual indication is provided to the device's user to indicate the updated security mode of operation (par. 65, lines 17-21).

17. As to claim 12, Schoen discloses a device where a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store (par. 30, lines 3-7).

18. As to claim 13, 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 (par. 30, lines 7-10).

19. As to claim 14, 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 (par. 73, lines 16-23; Schoen; claim 9, lines 4-7).

20. As to claim 15, Schoen discloses a method for use in establishing a security-related mode of operation for computing devices, comprising:

storing a security mode of operation in a policy data store (par. 69, lines 10-15);

sending the stored security mode of operation to the computing devices over a network (par. 73, lines 16-20);

where the sent security mode of operation places the computing devices into one or more predetermined security-related modes of operation (par. 69, line 13-15).

21. As to claim 16, Schoen discloses a method further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store (par. 60, lines 3-5).

22. As to claim 17, Schoen discloses 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 (par. 65, lines 17-21).

23. As to claim 18, Schoen discloses a method further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation (par. 66, lines 11-13; (par. 73, lines 16-23).

24. As to claim 20, Schoen discloses a digital signal containing the sent security mode of operation of claim 15 (par. 9, lines 3-6).

25. As to claim 21, Schoen discloses a computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15 (Schoen; claim 12, lines 1-3).

26. As to claim 22, Schoen discloses 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 (Schoen: claim 4, lines 1-5; par. 32, lines 3-7);

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 (par. 9, lines 1-6);

means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device (par. 65, lines 17-21).

Claim Rejections - 35 USC § 103

27. 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.

28. Claims 2, 3, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view of Wenocur et al. (US Patent Publication No. 2002/0165912 and Wencour hereinafter).

29. As to claim 2, 3, and 19 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).
>
> As to claim 19, Schoen discloses 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 19).

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 Wencour. Wencour discloses:

A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2) (par. 254, lines 1-13) to provide a secure mode of operation.

A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3) (par. 257, lines 1-7) to provide the means to utilize encryption.

As to claim 19, Schoen discloses 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 19) (par. 257, lines 1-7) to provide the means to utilize encryption.

Therefore, given the teachings of Wencour 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 features of Federal Information Processing Standard (FIPS) and Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) disclosed above by Wencour, for which secure mode will be enhanced (par. 257, lines 1-7).

Prior Art Made of Record

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kuroda (US Patent No. 5,935,248) Security level control apparatus and method for a network securing communications between parties without presetting the security level.

b. Freund (US Patent Publication No. 2004/0019807) System And Methodology For Providing Community-Based Security Policies.

c. Geiger et al. (US Patent No. 6,775,536) Method for validating an application for use in a mobile communication device.

d. Godfrey et al. (US Patent No. 7,317,699) System and method for controlling configuration settings for mobile communication devices and services.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN F. WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on Monday through Friday 7:30Am - 5:00Pm EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Benson can be reached on (571)272-2227. 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 F Wright/

Examiner, Art Unit 4158

/Walter Benson/
Supervisory Patent Examiner, Art Unit 4158

Notice of References Cited	Application/Control No. 11/065,901	Applicant(s)/Patent Under Reexamination ADAMS ET AL.
	Examiner BRYAN F. WRIGHT	Art Unit 4158 / Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,935,248	08-1999	Kuroda, Yasutsugu	726/14
*	B	US-2004/0019807	01-2004	Freund, Gregor P.	713/201
*	C	US-6,775,536	08-2004	Geiger et al.	455/411
*	D	US-7,317,699	01-2008	Godfrey et al.	370/328
*	E	US-2002/0165912	11-2002	Wenocur et al.	709/203
*	F	US-2003/0204722	10-2003	Schoen et al.	713/156
	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.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F WRIGHT	**Art Unit** 4158

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203		

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Index of Claims	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F WRIGHT	**Art Unit** 4158

✓	**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	01/30/2008								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								

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. 4175

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/065,901	02/25/2005 **RULE**	713	4158	555255012798

APPLICANTS

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

** **CONTINUING DATA** *************************

This appln claims benefit of 60/567,137 04/30/2004

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** **
06/01/2005

		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 /BRYAN F WRIGHT/ Examiner's Signature	□ Met after Allowance Initials	CANADA	10	22	4

ADDRESS

John V. Biernacki, Esq.
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, OH 44114
UNITED STATES

TITLE

System and method for configuring devices for secure operations

FILING FEE RECEIVED 1430	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

BIB (Rev. 05/07).

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	(2003/0204722)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:15
L2	1	("20030204722")	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:15
L3	1	l2 and (crypt$11 or encrypt $9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:18
L4	1	l2 and (read$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:21
L5	1	l2 and (media or medium)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:22
L6	0	l2 and (computer near (software or source or program))	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:24
L7	0	l2 and (computer same (software or source or program or code))	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:25
L8	1	l2 and (computer)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:25
L9	1	l2 and (stor$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:34
L10	1	l2 and (policy same security same state)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:37
L11	1	l2 and (notif$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:40
L12	1	l2 and (broadcast)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:48
L13	790	(726/1).ccls.	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:57
L14	5056062	@ad$<"20050225"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:58
L15	562	l13 and @ad $<"20050225"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 10:58

L16	0	"11065901"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 11:02
L17	1	"11/065901"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/30 11:02
S1	1	("6202157").pn.	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/28 17:08
S2	9	("6732168")	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/28 17:09
S3	47	("6202157")	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/28 17:09
S4	0	rothermel.pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/28 17:12
S5	329	rothermel.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/28 17:12
S6	1	00/69120	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/28 17:13
S7	3039673	WO 00/69120	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/28 17:14
S8	1	"WO 00/69120"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/28 17:14
S9	2199	(wireless and device and (policy or rule) and security and certificate and gateway and network and message and (mode or setting) and (transmit $9 and receiv$9))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:08
S10	1572	S9 and @ad<"20050225"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:08

S11	44470	S10 an FIPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:09
S12	56	S10 and FIPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:10
S13	70779	(establish$9 and security and (mode or setting) and device)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:48
S14	1023	S13 and FIPS	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:49
S15	21	S14 and (establish$9 same security same (mode or setting) same device)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:50
S16	921	S13 and (establish$9 same security same (mode or setting) same device)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:52
S17	638	S16 and @ad<"20050225"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:52
S18	286	S17 and (polic$9 or rule)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:54
S19	286	S18 and (security)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:56
S20	2	("7287269").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 08:59

S21	1	S20 and (polic$9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:00
S22	2	S20 and (security)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:04
S23	1	S20 and (security same polic$9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:05
S24	1	S20 and (security same operat$9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:06
S25	2	S20 and (level)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:13
S26	137	S19 and (security near (mode or level))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:17
S27	389	(security near relat$9 near (mode or operat$9 or level))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:33
S28	291	S27 and @ad<"20050225"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 09:33
S29	0	"11065901"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 09:51
S30	1	"11/065901"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 09:51
S31	394115	(policy or rule)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 10:57
S32	416455	(polic$9 or rule)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 10:57

S33	128466	S32 and (secur$9 or security)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 10:58
S34	127840	S33 and (mode or setting or state or method or form or plan or style or technique or config$9 or version)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 11:00
S35	125820	S34 and (function or operat$9 or perform$9 or utiliz$9 or usance or value)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 11:03
S36	108974	S35 and (stor$9 or reposit $9 or database or central $9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 11:06
S37	108713	S36 and (establish$9 or determin$9 or identif$9 or install$9 or download$9 or upload$9 or origin$9 or (set near up) or form or provid$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 11:10
S38	84595	S37 and @ad<"20050225"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 11:11
S39	84557	S38 and (relat$9 or correlat$9 or interchang$9 or parallel or link$9 or correspond$9 or depend $9 or affiliat$9 or associat $9 or equivalent of match $9 compar$9 or analogous or concurrent or allied or duplicat$9 or equal$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 11:16
S40	2	S19 and ((display or visual $9) near secur$9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 11:42
S41	153	S19 and ((display or visual $9) same secur$9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 11:42
S42	2	("7287269").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 12:21
S43	1	S42 and display	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 12:22

S44	37	S41 and (visual same (setting or mode or operation))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 12:24
S45	41	S41 and (visual$9 same (setting or mode or operation))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 12:24
S46	23	S41 and (visual$9 same secur$9 same (setting or mode or operation))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/29 12:27
S47	0	("2003024722")	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:30
S48	0	("2003/024722")	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:30
S49	1	("7317699").pn.	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:32
S50	1	S49 and (secur$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:33
S51	5	("5935248").pn. or ("20030204722") or ("7317699").pn. or ("6775536").pn. or ("20040019807")	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:38
S52	5	S51 and display	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:38
S53	5	S51 and (polic$9 or rule)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:40
S54	5	S51 and ((polic$9 or rule) same secur$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:46
S55	1	S51 and (secur$ same mode same operat$8)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:49
S56	5	S51 and (secur$ same operat$8)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 12:49
S57	5	S51 and (transmit$9 or sending or send)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 13:47

S58	5	S51 and (display)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 13:51
S59	1	S51 and (visual)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 13:52
S60	0	S51 and (FIPS and (AES or 3DES))	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 15:52
S61	539	(FIPS and (AES or 3DES))	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 15:52
S62	376	S61 and @ad<"20050225"	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 15:52
S63	344	S62 and (security or secur $9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 15:53
S64	157	S63 and (policy or policies or rule)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 15:54
S65	9	S64 and S16	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 15:55
S66	5	S51 and (device)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 16:24
S67	3	S51 and (device and desktop)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 16:24
S68	3	(2003/0204722)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 17:32
S69	5	S58 and (chang$9 or modif $9 or updat$9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 17:34
S70	3	S58 and ((chang$9 or modif$9 or updat$9) same (policy or policies or rule))	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 17:36
S71	4	S58 and (digital)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 17:51
S72	5	S58 and secur$5	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 17:55
S73	5	S58 and receiv$9	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 18:01
S74	1	S58 and (reply or acknow $9)	US-PGPUB; USPAT; IBM_TDB	OR	ON	2008/01/29 18:06

S75	5	S58 and (reply or acknow $9 or respon$9)	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:07

S76	1	S58 and visual$9	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:09

S77	4	S58 and interface	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:21

S78	4	S58 and (interface same (policies or policy or rule))	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:23

S79	5	S58 and (process$9)	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:27

S80	5	S58 and (process$9 same secur$9)	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:33

S81	1	S58 and (process$9 same secur$9 same state)	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:37

S82	5	S58 and (secur$9 same (polic$5 or rule))	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:41

S83	3	S58 and (plurality same device)	US-PGPUB;
			USPAT;
			IBM_TDB
				OR	ON	2008/01/29 18:55

1/30/2008 11:04:57 AM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. 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 contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	11/065,901
Filing Date	February 25, 2005
First Named Inventor	Neil P. Adams
Art Unit	~~Not Yet Assigned~~ 4158
Examiner Name	~~Not Yet Assigned~~ Bryan Wright
Attorney Docket Number	555255012798

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/B.W./		US- 6202157 B1	03-13-2001	Brownlie, et al.	
/B.W./		US- 6732168 B1	05-04-2004	Bearden, et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
/B.W./		WO 0069120 A1	11-16-2000			□
						□
						□
						□
						□
						□

Examiner Signature	/Bryan Wright/	Date Considered	01/30/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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/08B (08-03)
Approved for use through 07/31/2006. 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 contains a valid OMB control number.

Substitute for form 1449/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application Number**	11/065,901
				Filing Date	February 25, 2005
				First Named Inventor	Neil P. Adams
(Use as many sheets as necessary)				Art Unit	~~Not Yet Assigned~~ 4158
				Examiner Name	~~Not Yet Assigned~~ Bryan Wright
Sheet	2	of	2	Attorney Docket Number	555255-012798

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/B.W./		International Search Report of Application No. PCT/CA2005/000294, date of mailing June 20, 2005 - 11 pgs	

Examiner Signature	/Bryan Wright/	Date Considered	01/30/2008

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

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 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 2 hours 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, 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.

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	4158
Examiner	:	Bryan F. Wright

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSIVE AMENDMENT

Dear Sir:

Please amend the application as indicated and consider the following remarks. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

IN THE CLAIMS

1. (Currently Amended) 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 computing devices over a network;

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

wherein at least one of the plurality of ~~the~~ 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 ~~device's~~ user of the one of the plurality of computing devices.

2. (Original) The system of claim 1, wherein the secure 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. (Currently Amended) The system of claim 1, ~~wherein an administrator uses an interface to update~~ further comprising an administrator interface for updating the configuration data related to a plurality of computing devices that is stored in the policy data store[[,]] and ~~uses an interface to communicate~~ for communicating security modes of operation to the computing devices;

wherein 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;

wherein the policy data store stores IT security policies related to the 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.

7. (Original) The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Currently Amended) 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 secure 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.

9. (Original) The device of claim 8, 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.

10. (Currently Amended) The ~~system~~ device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. (Original) The device of claim 10, 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.

12. (Currently Amended) The device of claim 11, ~~wherein a company or government administrator uses~~ further comprising an administrator interface ~~to change~~ for changing the configuration data stored on the centralized policy data store.

13. (Original) The device of claim 8, 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.

14. (Original) The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Currently Amended) A method for use in establishing a security-related mode of operation for a computing device~~s~~, comprising:

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

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

wherein the sent security mode of operation places the computing device~~s~~ into ~~one or more~~ a predetermined security-related mode~~s~~ 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.

16. (Original) The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. (Currently Amended) The method of claim 15, further comprising the step of displaying the security mode of operation of ~~a~~ the computing device by providing a visual indication on a screen of the computing device.

18. (Currently Amended) The method of claim 15, further comprising the step of receiving an indication that the device~~s have~~ has received and entered into the sent security mode of operation.

19. (Original) The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. (Original) A digital signal containing the sent security mode of operation of claim 15.

21. (Original) Computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15.

22. (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.

23. (New) 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.

IN THE ABSTRACT

Please delete the abstract and replace it with the new abstract which is included with this amendment on a separate sheet of paper pursuant to MPEP 608.01(b) and 37 C.F.R. § 1.72(b).

ABSTRACT

Systems and methods for establishing a security-related mode of operation for computing devices. A security-related mode of operation is established through security mode configuration data. The security mode configuration data specifies the proper security mode or modes for operation of the computing devices.

REMARKS

Claims 1-22 are pending in the instant application and stand rejected. New claim 23 has been added herein. Assignee respectfully traverses the rejections of the pending claims.

Objections to Drawings

The office action objected to figures 1 and 2 of the instant application. Specifically, the office action stated that reference items 15, 25, and 95 in figure 1 and reference items 15, 25, 50, 80, and 100 in figure 2 "are missing identification labels." 37 C.F.R. 1.83 states the law regarding the content of drawings in a patent application. Subsection (a) of 37 C.F.R. 1.83 reads:

> The drawing in a nonprovisional application must show every feature of the invention specified in the claims. However, conventional features disclosed in the description and claims, where their detailed illustration is not essential for a proper understanding of the invention, ***should be illustrated in the drawing in the form of a graphical drawing symbol or a labeled representation*** (e.g., a labeled rectangular box). (Emphasis added.)

As the highlighted portion makes clear, when a drawing contains a "conventional feature" that does not need to be illustrated in detail to understand the invention, that feature may be illustrated as a graphical drawing symbol **or** as a labeled representation. For example, in the instant application reference number 15 depicts an e-mail message. Both the concept of an e-mail message and the graphical drawing symbol used to represent an e-mail message in figures 1 and 2 would be well-known to one having ordinary skill in the art. This also is true of reference number 80 in figure 2, which depicts a re-enveloped e-mail message. Because the graphical drawing symbols for the conventional features depicted in figures 1 and 2 would be well-known to one having ordinary skill in the art, assignee respectfully submits that figures 1 and 2 comply with the law, as stated in 37 C.F.R. 1.83, and asks that the objection to the drawings be withdrawn.

Objections to Specification

Assignee has provided herein a replacement Abstract for the instant application. Assignee respectfully submits that the replacement Abstract provided herein complies with the requirements for proper content of an Abstract and therefore requests that the objection to the Abstract set forth in the office action be withdrawn.

Claim Rejections – 35 U.S.C. § 112

Claim 22 stands rejected under 35 U.S.C. § 112, sixth paragraph as failing to conform to proper means-plus-function claiming structure. As support for this rejection, the office action cites *Ex parte Klumb*, 159 U.S.P.Q. 694 (Bd. App. 1967). In *Klumb*, the examiner rejected the applicant's claim as being indefinite under 35 U.S.C. § 112. *Id.* The applicant's claim language recited "a plate means" and "a wing means" ***without specifying any function*** of the recited means. *Id.* at 695. The Patent Office Board of Appeals further stated that "expressions, such as 'means for printing' or 'printing means,' would have the same connotations and both would be in conformity with the statute." *Id.* However, the Board rejected the applicant's argument that the words "plate" and "wing" specified the functions, stating:

> [T]he terms "plate" and "wing," as modifiers of the structureless term "means," specify no function to be performed, as is self-evident if one attempts to recast into the alternative grammatical form of "means for plating" or "means for winging," which of course are obviously not pertinent to the instant disclosure. *Id.*

Claim 22 of the instant application, on the other hand, ***does specify a function*** for each of the means recited in the claim. For example, claim 22 recites the function of displaying the security mode of operation to a user of the computing device for one of its means-plus-function elements. The other elements of claim 22 are similarly clear in specifying the function associated with the means they recite. Assignee notes that *Klumb* actually supports assignee's position with respect to claim 22 – in other words, in contrast to the claim language at issue in *Klumb*, the language of claim 22 does specify functions within the means-plus-function limitations and thus does not fail for indefiniteness under 35 U.S.C. § 112, sixth paragraph. Therefore, the rejection of claim 22 should be withdrawn.

Claim Rejections – 35 U.S.C. §§ 102, 103

Claims 1, 4-18, and 20-22 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0204722, application of Schoen, et al. (Schoen). Claims 2-3 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of U.S. Publication No. 2002/0165912, application of Wenocur, et al. (Wenocur). Assignee respectfully disagrees with the rejections.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. Claim 1 recites that the computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, where the output is configured to comprise a visual indication of the security mode of operation to the user of the device. As support in assignee's specification for this feature, the specification describes that at step 404 in figure 6, the devices receive a deployed security mode command and process the security mode command. Further, processing of the command causes the devices to operate in the defined security mode. Once the devices are operating in the defined modes, at step 406, a user of the device can see an indication of which specific security mode the device is operating in.

In rejecting claim 1, the office action cites paragraph 65, lines 17-21 of Schoen as disclosing this aspect. The passage from Schoen cited in the office action reads:

> The instant messaging secured public key infrastructure proxy may add text to an instant message packet that provides visual indications of the

> ***results*** of the secure processing such as background display changes, signing the message, or other operations. (Emphasis added.)

As this passage states, the visual indication disclosed in Schoen is used to provide a visual indication of the results of secure processing of an instant message packet. This teaching from Schoen does not disclose the recited feature of claim 1, which is directed to providing a visual indication of the ***security mode*** in which a device is operating. Given this lack of disclosure, Schoen does not anticipate the subject matter of claim 1 of the instant application. Thus, claim 1 is allowable for at least this reason and should proceed to issuance.

Assignee disagrees with other positions in the office action as well. For example, claim 4 of the instant application recites a first security mode data structure including a first security mode associated with a first plurality of computing devices and a second security mode data structure including a second security mode associated with a second plurality of computing devices. Support for this subject matter is found, for example, in figure 9 of the instant application. Figure 9 shows at 610 and 620 two distinct security mode settings, Mode A and Mode B. Further, at 700 and 710, figure 9 depicts that one example mobile device receives the Mode A settings while another example mobile device receives the Mode B settings. In rejecting claim 4, the office action cites lines 16-23 of paragraph 73 of Schoen. The cited passage reads:

> Administrators create the instant messaging policy certificates and are created as noted above at a central point and published to a repository or broadcast to ***active instant messaging subscribers*** if desired. As operating conditions change, a new instant messaging PKI policy certificate is published. At the option of the administrator, ***all active instant messaging devices*** may be notified that a new certificate is available. (Emphasis added.)

The cited paragraph discloses an optional notification to all instant messaging devices that a new certificate is available. This is not teaching the subject matter of claim 4. Nothing in the cited paragraph from Schoen discloses a first plurality of computing devices and a second plurality of computing devices that receive different security modes, as required by claim 4 (e.g., Mode A settings are sent to one example mobile device, while Mode B settings are sent to another example mobile device). For at least these reasons, claim 4 is patentable over Schoen and should proceed to issuance.

New dependent claim 23 has been added herein. Claim 23, which depends from claim 5, recites that 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 requires use of AES encryption and that 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 requires use of Triple DES encryption. Assignee respectfully submits that nothing in the cited references discloses the subject matter of new claim 23 and that claim 23 therefore is allowable and should proceed to issuance.

Independent claims 8, 15, and 22 also were rejected based upon the Schoen reference. Claims 8 and 15 have been amended herein and claims 8, 15, and 22 recite subject matter analogous to that of claim 1. Given that claims 8, 15, and 22 recite subject matter analogous to the subject matter of claim 1, and that the subject matter is not disclosed by Schoen, these claims are allowable for at least the reasons set forth above with respect to claim 1. Therefore, claims 8, 15, and 22 should proceed to issuance.

It should be noted that assignee has not presented arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to assignee's right to present arguments to all of the dependent claims at any point in the future. In addition, because each of the dependent claims depends from a base claim that is itself allowable, the dependent claims are allowable for at least these reasons and should proceed to issuance.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

By:____________________

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point; 901 Lakeside Avenue
Cleveland, OH 44114
(216) 586-3939

Electronic Patent Application Fee Transmittal

Application Number:	11065901
Filing Date:	25-Feb-2005
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:	555255012798
Filed as Large Entity	

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	1	50	50
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**50**

Electronic Acknowledgement Receipt

EFS ID:	3260251
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
Title of Invention:	System and method for configuring devices for secure operations
First Named Inventor/Applicant Name:	Neil P. Adams
Correspondence Address:	John V. Biernacki, Esq. JONES DAY North Point 901 Lakeside Avenue Cleveland OH 44114 US 2165863939 -
Filer:	Stephen D. Scanlon/Debra Pejeau
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255012798
Receipt Date:	06-MAY-2008
Filing Date:	25-FEB-2005
Time Stamp:	13:55:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$50

RAM confirmation Number	7707
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		012798_Amendment.pdf	480838 51388880c9aee077cb5001ebb59d6ac097b0cc20	yes	16

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment - After Non-Final Rejection	1	1
Claims	2	8
Abstract	9	10
Applicant Arguments/Remarks Made in an Amendment	11	16

Warnings:

Information:

2	Fee Worksheet (PTO-06)	fee-info.pdf	8154 ac1732189a6b72dc28bc1dcb9c83288a1275306d	no	2

Warnings:

Information:

Total Files Size (in bytes):	488992

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.

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 11/065,901	Filing Date 02/25/2005	□ 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	**05/06/2008**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 22	Minus	** 22	= 0	X $ =		OR	X $50=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $210=	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:
/EVELYN G. NIMMONS/

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

7590 07/22/2008

John V. Biernacki, Esq.
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
07/22/2008	PAPER

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.

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 11/065,901	**Applicant(s)** ADAMS ET AL.	
	Examiner BRYAN WRIGHT	**Art Unit** 2131	

-- 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 *29 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ 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

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2005* 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).

11)☐ 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

12)☐ 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 _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

FINAL ACTION

1. Amendment A has been entered into record.

2. Claim 23 added. Claims 1-23 are pending

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> **(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21 (2) of such treaty in the English language.**

3. Claims 1,4-18, and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Schoen et al. (US Patent Publication No. 2003/0204722 and Schoen hereinafter).

4. As to claims 1, 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 security mode data structure stores a security mode of operation (par. 69, line 13-15); **where the stored security mode of operation is provided to the computing devices over a network** (par. 73, lines 16-20); **where the security mode of operation places the computing devices in a predetermined security mode of operation** (par. 69, line 13-15); **where the 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** (par. 65, lines 17-21).

5. 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).

6. 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).

7. 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).

8. As to claim 7, 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).

9. As to claim 8, Schoen discloses 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 (par. 69, lines 21-32);

and a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (Schoen; claim 10, lines 2-5);

where 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 (Schoen: claim 9, lines 4-7).

10. As to claim 9, Schoen discloses a **device where 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** (par. 65, lines 17-21).

11. As to claim 10, Schoen discloses a **system where the visual indication of the security mode is provided by a security options screen** (par. 65, lines 17-21).

12. As to claim 11, Schoen discloses a **device where the 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. 30, lines 3-7), **where a visual indication is provided to the device's user to indicate the updated security mode of operation** (par. 65, lines 17-21).

13. As to claim 12, Schoen discloses a **device where a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store** (par. 30, lines 3-7).

14. As to claim 13, 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** (par. 30, lines 7-10).

15. As to claim 14, 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** (par. 73, lines 16-23; Schoen; claim 9, lines 4-7).

16. As to claim 15, Schoen discloses a **method for use in establishing a security-related mode of operation for computing devices, comprising:**

storing a security mode of operation in a policy data store (par. 69, lines 10-15);

sending the stored security mode of operation to the computing devices over a network (par. 73, lines 16-20);

where the sent security mode of operation places the computing devices into one or more predetermined security-related modes of operation (par. 69, line 13-15).

17. As to claim 16, Schoen discloses a **method further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store** (par. 60, lines 3-5).

18. As to claim 17, Schoen discloses 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** (par. 65, lines 17-21).

19. As to claim 18, Schoen discloses a **method further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation** (par. 66, lines 11-13; (par. 73, lines 16-23).

20. As to claim 20, Schoen discloses a **digital signal containing the sent security mode of operation of claim 15** (par. 9, lines 3-6).

21. As to claim 21, Schoen discloses a **computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15** (Schoen; claim 12, lines 1-3).

22. As to claim 22, Schoen discloses 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 (Schoen: claim 4, lines 1-5; par. 32, lines 3-7);

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 (par. 9, lines 1-6);

means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device (par. 65, lines 17-21).

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.

23. Claims 2, 3, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view of Wenocur et al. (US Patent Publication No. 2002/0165912 and Wencour hereinafter).

24. As to claim 2, 3, and 19 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 19).

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 Wencour. Wencour discloses:

A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2) (par. 254, lines 1-13) to provide a secure mode of operation.

A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3) (par. 257, lines 1-7) to provide the means to utilize encryption.

> **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 19) (par. 257, lines 1-7) to provide the means to utilize encryption.

Therefore, given the teachings of Wencour 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 features of Federal Information Processing Standard (FIPS) and Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) disclosed above by Wencour, for which secure mode will be enhanced (par. 257, lines 1-7).

25. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view of Lord et al. (US Patent No. 7,131,003 and Lord hereinafter).

26. As to claim 23, the system disclose by Schoen shows substantial features of the claimed invention (discussed in the paragraphs above), It fails to disclose:

> **A system where 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** (claim 23);

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 Lord. Lord discloses:

> **A system where 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** (claim 23) (for purposes of policy (i.e., **first security mode data structure**) cryptographic operations Load provides FIPS capability [col. 5, lines 5-15] such that modification of Schoen teachings of AES and DES encryption provides enhanced security policy related operations);

Therefore, given the teachings of Lord, 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 features of FIPS cryptographic operations disclosed above by Lord, for which security policy related operations will be enhanced [col. 5, lines 5-15].

Response to Arguments

27. Examiner withdraws Objection to Drawings in view of applicant's argument.

28. Examiner withdraws Objection to Specification in view of applicant's submittal of a replacement Abstract.

29. Applicant's arguments filed May, 6, 2008 have been fully considered but they are not persuasive. Examiner draws applicant attention to submittal below.

30. Applicant's argument, "***As this passage states, the visual indication disclosed in Schoen is used to provide a visual indication of the results of secure processing of an instant message packet. This teaching from Schoen does not disclose the recited feature of claim 1, which is directed to providing a visual indication of the security mode in which a device is operating. Given this lack of disclosure, Schoen does not anticipate the subject matter of claim 1 of the instant application. Thus, claim 1 is allowable for at least this reason and should proceed to issuance.***

Examiner respectfully submits while the cited paragraph, line or figure may not construe said "security mode" as a whole, applicant is respectfully reminded that applicant is responsible for the reference as whole. Examiner, further respectfully submits claim interpretation is performed as such, " pending claims must be given their broadest reasonable interpretation consistent with the specification [MPEP 2111]. As such, Examiner draws applicant's attention to applicant's specification, paragraph [0039] for which applicant recites, " ***… 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.***", specifically ", **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."** is representative of a policy base communication. Those skilled in the art would recognize the use of policies as such to maintain behavioral instructions thereby permitting the controlling of a particular device. Notwithstanding, these policies are often deployed to reside on the device and as such configure the device as necessitated. Therefore, the "**security mode**" as prescribed in applicant’s specification is readily taught by the Schoen reference, specifically paragraph [0069].

31. Applicant's argument, “***Assignee disagrees with other positions in the office action as well. For example, claim 4 of the instant application recites a first security mode data structure including a first security mode associated with a first plurality of computing devices and a second security mode data structure including a second security mode associated with a second plurality of computing devices. Support for this subject matter is found, for example, in figure 9 of the instant application. Figure 9 shows at 610 and 620 two distinct security mode settings, Mode A and Mode B. Further, at 700 and 710, figure 9 depicts that one example mobile device receives the Mode A settings while another example mobile device receives the Mode B settings. In rejecting claim 4, the office action cites lines 16-23 of paragraph 73 of Schoen. The cited passage reads:”***

Examiner respectfully submits while the cited paragraph, line or figure may not construe said “security mode” as a whole, applicant is respectfully reminded that applicant is responsible for the reference as whole. Examiner, further respectfully submits claim interpretation is performed as such, “ pending claims must be given their broadest reasonable interpretation consistent with the specification” [MPEP 2111]. As such examiner respectfully draws applicant’s attention to Schoen reference, specifically [0069], lines 9-20. Schoen teaches control data (i.e., enable/disable) in the context of controlling operation. Furthermore, relative to security related operation (i.e., **Security Mode**), Schoen distinctively teaches policy control data for which security related operations are inclusive.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

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, AYAZ Sheikh can be reached on (571)272-3795. 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 2131
/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131

Notice of References Cited	Application/Control No. 11/065,901	Applicant(s)/Patent Under Reexamination ADAMS ET AL.	
	Examiner BRYAN WRIGHT	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,131,003	10-2006	Lord et al.	713/168
	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.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F WRIGHT	**Art Unit** 2131

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203		
Additional search class/subclass 713/168	7/18/2008	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Index of Claims

Application/Control No. 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
Examiner BRYAN F WRIGHT	**Art Unit** 2131

✓	**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	01/30/2008	07/18/2008							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23		✓							

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13
S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$.DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30
S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40

S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46
S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51
S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45

7/18/2008 8:25:56 AM
C:\Documents and Settings\bwright\My Documents\EAST\Workspaces\11065901.wsp

PTO/SB/30 (12-08)
Approved for use through 01/31/2009. 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 contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/065,901
Filing Date	February 25, 2005
First Named Inventor	Neil P. Adams
Art Unit	4175
Examiner Name	Bryan F. Wright
Attorney Docket Number	555255-012798

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

a. □ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

i. □ Consider the arguments in the Appeal Brief or Reply Brief previously filed on ______

ii. □ Other ______

b. ☑ Enclosed

I. ☑ Amendment/Reply

ii. □ Affidavit(s)/ Declaration(s)

iii. □ Information Disclosure Statement (IDS)

iv. □ Other ______

2. Miscellaneous

a. □ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of ______ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

b. □ Other ______

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

a. ☑ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 50-1432.

i. ☑ RCE fee required under 37 CFR 1.17(e)

ii. ☑ Extension of time fee (37 CFR 1.136 and 1.17)

iii. □ Other ______

b. □ Check in the amount of $ ______ enclosed

c. □ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	January 21, 2009
Name (Print/Type)	John V. Biernacki	Registration No.	40,511

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. 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: Mail Stop RCE, 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.

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	4158
Examiner	:	Bryan F. Wright

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSIVE AMENDMENT

Dear Sir:

Please amend the application as indicated and consider the following remarks. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

IN THE CLAIMS

1. (Previously Presented) 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 computing devices over a network;

wherein the security mode of operation places the 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.

2. (Original) The system of claim 1, wherein the secure 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. (Previously Presented) The system of claim 1, further comprising an administrator interface for updating the configuration data related to a plurality of computing devices that is stored in the policy data store and for communicating security modes of operation to the computing devices;

wherein 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;

wherein the policy data store stores IT security policies related to the 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.

7. (Original) The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Previously Presented) 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 secure 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.

9. (Original) The device of claim 8, 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.

10. (Previously Presented) The device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. (Original) The device of claim 10, 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.

12. (Previously Presented) The device of claim 11, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

13. (Original) The device of claim 8, 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.

14. (Original) The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Previously Presented) 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.

16. (Original) The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. (Previously Presented) The method of claim 15, 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.

18. (Previously Presented) The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. (Original) The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. (Original) A digital signal containing the sent security mode of operation of claim 15.

21. (Original) Computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15.

22. (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.

23. (Previously Presented) 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.

24. (New) 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.

<u>REMARKS</u>

Claims 1-23 are pending in the instant application and stand rejected. New claim 24 has been added herein. Assignee respectfully traverses the rejections of the pending claims.

Claim Rejections – 35 U.S.C. §§ 102, 103

Claims 1, 4-18, and 20-22 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0204722, application of Schoen, et al. (Schoen). Claims 2-3 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of U.S. Publication No. 2002/0165912, application of Wenocur, et al. (Wenocur). Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of U.S. Patent No. 7,131,003 (Lord). Assignee respectfully disagrees with the rejections.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. Claim 1 specifically recites that the computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, where the output is configured to comprise a ***visual indication of the security mode of operation <u>to the user</u> of the device***. This allows a user of the device to see an indication of which specific security mode the device is operating in.

In rejecting this feature of claim 1, the office action cites paragraph 69 of Schoen. This passage from Schoen cited in the office action reads:

> [0069] FIG. 9 diagramatically illustrates one example of an instant messaging PKI policy certificate 706. For purposes of simplicity, it will be understood that the instant messaging PKI policy certificate 706 includes conventional certificate data in addition to the new instant messaging PKI policy control data described herein. For example, though not shown, an issuance date and validity period may be set forth in the instant messaging PKI policy certificate 706 along with other information. In this example, the instant messaging PKI policy certificate 706 includes instant messaging PKI policy control data 900 for one or more instant messaging subscribers, which includes security and non-security related operations

> data 902 and 903 and data that defines a selected operation state, generally designated at 904, for each of the security related operations. It will be recognized that this is only an example and, fewer, more or different instant messaging policy control data may be used if desired. For example, one security related operation may be to allow an instant messaging originator to digitally sign instant messages as indicated by security related operation data 906. An administrator, through a graphic user interface at the instant messaging PKI policy certificate unit 700, may designate that a particular instant messaging originator may be prohibited from signing instant messages or may permit the instant messaging originator to digitally sign messages or allow the user to configure locally whether the user wishes to digitally sign instant messages. A similar defined operation state 904 may be set forth to allow communication with unsecure instant messaging clients as indicated by security related operation data 908, allow unsecure file transfers as indicated by security related operation data 910 or any other suitable security related operations. Other examples shown include allowing or setting a public key cryptographic signature algorithm as shown by security related operation data 912 to one of CAST, DES or AES, or any other suitable cryptographic signature algorithm. In addition, the security related operation data 902 may indicate the TCP port permitted for the secure instant messaging PKI proxy as shown by security related operation data 914. The instant messaging PKI policy certificate 706 includes the digital signature 916 of the instant messaging PKI policy server and therefore is a trusted instant messaging policy enforcement mechanism.

This passage from Schoen discloses that a particular instant messaging originator may be permitted or prohibited from certain operations, such as being permitted to sign instant messages or may permit the instant messaging originator to digitally sign messages. However, Schoen does not disclose the aforementioned feature of claim 1, which is directed to providing to the user a visual indication of the ***security mode*** in which the computing device (that receives the security mode of operation and which is to be placed in a predetermined security mode of operation) is operating. Schoen may disclose permitting or prohibiting certain operations, but this does not operate as a disclosure of the specific claimed feature of a visual indicator being provided to the user of a device which has been placed in a particular security mode. Given this lack of disclosure, Schoen does not anticipate the subject matter of claim 1 of the instant application. Thus, claim 1 is allowable for at least this reason and should proceed to issuance.

New claim 24 has been added herein. Claim 24 recites that 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. Support for this new claim is found in assignee's specification, such as in the description of reference numeral 230 of figure 3 of assignee's specification. None of the cited references disclose such limitations of claim 24. For example, paragraph 69 of Schoen does not disclose that a computing device receives a disable message for disabling the security mode of operation. Instead, Schoen discloses various PKI policy controls for permitting or prohibiting certain operations, such as being permitted to sign instant messages or may permit the instant messaging originator to digitally sign messages. There is no disclosure of the limitations of claim 24. Accordingly, claim 24 is allowable and should proceed to issuance.

Independent claims 8, 15, and 22 also were rejected based upon the Schoen reference. Claims 8, 15, and 22 recite subject matter analogous to that of claim 1. Given that claims 8, 15, and 22 recite subject matter analogous to the subject matter of claim 1, and that the subject matter is not disclosed by Schoen, these claims are allowable for at least the reasons set forth above with respect to claim 1. Therefore, claims 8, 15, and 22 should proceed to issuance.

It should be noted that assignee has not presented arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to assignee's right to present arguments to all of the dependent claims at any point in the future. In addition, because each of the dependent claims depends from a base claim that is itself allowable, the dependent claims are allowable for at least these reasons and should proceed to issuance.

[Continued on the next page]

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Date: January 21, 2009

Respectfully submitted,

By: John Biernacki
John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point; 901 Lakeside Avenue
Cleveland, OH 44114
(216) 586-3939

Electronic Patent Application Fee Transmittal

Application Number:	11065901
Filing Date:	25-Feb-2005
Title of Invention:	System and method for configuring devices for secure operations
First Named Inventor/Applicant Name:	Neil P. Adams
Filer:	Stephen D. Scanlon/John V. Biernacki
Attorney Docket Number:	555255012798

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:				
Claims in excess of 20	1202	1	52	52
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1110	1110
Miscellaneous:				
Request for continued examination	1801	1	810	810
			Total in USD ($)	**1972**

Electronic Acknowledgement Receipt

EFS ID:	4644061
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
Title of Invention:	System and method for configuring devices for secure operations
First Named Inventor/Applicant Name:	Neil P. Adams
Correspondence Address:	John V. Biernacki, Esq. JONES DAY North Point 901 Lakeside Avenue Cleveland OH 44114 US 2165863939 -
Filer:	Stephen D. Scanlon/John V. Biernacki
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255012798
Receipt Date:	21-JAN-2009
Filing Date:	25-FEB-2005
Time Stamp:	09:58:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1972

RAM confirmation Number	16392
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	Extension of Time	DOC046.pdf	58128 0b3f3fc1991661881bb5bffaaa41d68d1e1c3808	no	1
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	DOC045.pdf	71143 1585e46420c70794227711c622d26df46b399427	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3	Amendment Submitted/Entered with Filing of CPA/RCE	DOC047.pdf	390192 e2a27b8d6b8d5bfd824ec01528fdca12df2f430c	no	11
Warnings:					
Information:					
4	Fee Worksheet (PTO-06)	fee-info.pdf	33826 cfef0667b028341a623ea8d73fb8532b9c922011	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	553289		

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.

PTO/SB/22 (12-08)
Approved for use through 01/31/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE
Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** ***(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)***	Docket Number (Optional) 555255-012798
Application Number 11/065,901	Filed February 25, 2005
For System and Method for Configuring Devices for Secure Operations	
Art Unit 4175	Examiner Bryan F. Wright

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	
□ One month (37 CFR 1.17(a)(1))	$130	$65	$
□ Two months (37 CFR 1.17(a)(2))	$490	$245	$
☑ Three months (37 CFR 1.17(a)(3))	$1110	$555	$ 1,110.00
□ Four months (37 CFR 1.17(a)(4))	$1730	$865	$
□ Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

□ Applicant claims small entity status. See 37 CFR 1.27.

□ A check in the amount of the fee is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-1432 .

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the □ applicant/inventor.

□ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration Number 40,511

□ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 ______________

Signature

January 21, 2009
Date

John V. Biernacki
Typed or printed name

(216) 586-7747
Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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/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 11/065,901	Filing Date 02/25/2005	□ 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))							
			TOTAL			TOTAL	

* 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	**01/21/2009**	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	** 22	= 2	X $ =		OR	X $52=	104
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	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	**104**

		(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:
/JACQULYN L. WILLIAMS/

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.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 01/26/2009

```
JWILLIA1     SALE   #00000003     Mailroom Dt:  01/21/2009     501432    11065901
                     01      FC : 1202                    52.00  DA
```

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Adams et al
Title	:	System and Method for Configuring Devices …
Application No.	:	11/065,901
Filing Date	:	2/25/05
Confirmation No.	:	4175
Examiner	:	Bryan F. Wright
Group Art Unit	:	2131
Attorney Docket	:	555255012798

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

In compliance with 37 CFR 1.56, a list of documents is set forth on the attached Form PTO-1449. Copies of the documents are enclosed.

The documents include a Supplementary European Search Report for European Patent App. No. 05714536, which is related to the present application, and a reference cited in the Search Report.

Under 37 CFR 1.97(b)(3), no fee is due for this Statement, because it is submitted before a first office action after an RCE (Request for Continued Examination). However, if any fee is due, it should be charged to the Jones Day Deposit Account No. 50-1432, Reference No. 555255012798.

Respectfully submitted,

Mitchell Rose

Mitchell Rose (Reg. No. 47,906)
JONES DAY
901 Lakeside Ave.
Cleveland, OH 44114
(216)586-7094

1/26/09

FORM PTO-1449 (Modified) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	Atty Docket No.: 555255012798
	Application No.: 11/065,901
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary)	Applicant: Adams et al
	Filed: 2/25/05
(37 CFR 1.98(b))	Group: 2131

U.S. PATENT DOCUMENTS

Exam. Init.		Patent Number	Issue/Publ Date	Patentee	Class	Sub-class	Filing Date

FOREIGN PATENT OR PUBLISHED FOREIGN PATENT APPLICATION

							Translation	
Exam. Init.		Document Number	Publication Date of Grant	Country or Patent Office	Class	Sub-class	Yes	No

OTHER DOCUMENTS (Including Author, Title, Date**, Relevant pages, Place of Publication***)

		Supplementary European Search Report, issued 7/11/07 by European Patent Office, for European Patent App. No. 05714536
		S. Gavrila et al, "Assigning and Enforcing Security Policies on Handheld Devices", Canadian Information Technology Security Symposium, 5/17/02, pages 0-7, XP002440113

Examiner	Date Considered

EXAMINER: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Acknowledgement Receipt

EFS ID:	4673183
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
Title of Invention:	System and method for configuring devices for secure operations
First Named Inventor/Applicant Name:	Neil P. Adams
Correspondence Address:	John V. Biernacki, Esq. JONES DAY North Point 901 Lakeside Avenue Cleveland OH 44114 US 2165863939 -
Filer:	Stephen D. Scanlon/Mitchell Rose
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255012798
Receipt Date:	26-JAN-2009
Filing Date:	25-FEB-2005
Time Stamp:	13:16:28
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	NPL Documents	RIM798IDSdocGavrila.pdf	943634 910676adb60832c3aa6edc9090283fc429a73e54	no	8
Warnings:					
Information:					
2	Foreign Reference	RIM798IDSdocSESRfor05714536.pdf	120292 6de0924c29c4fd1bb2830cc4d471e07c288feca5	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Filed (SB/08)	DOC053.pdf	69098 236d5c4a91188ca196a8f4a62bc488b5f9d21530	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
		Total Files Size (in bytes):	1133024		

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.

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

7590 03/30/2009

John V. Biernacki, Esq.
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/30/2009	PAPER

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.

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 11/065,901	**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 *1/25/2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ 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).

11)☐ 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

12)☐ 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 *1/26/2009*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/21/2009 has been entered. Claim 24 is new. Claim 1-24 are pending.

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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 1, 4-18, and 20-22 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 Marty Sems (NPL "Verifying Identity In A Digital World" and Sems hereinafter).

2. As to claims 1, 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 security mode data structure stores a security mode of operation (par. 69, line 13-15);

where the stored security mode of operation is provided to the computing devices over a network (par. 73, lines 16-20);

where the security mode of operation places the computing devices in a predetermined security mode of operation (par. 69, line 13-15);

where at least on 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 Sems. Sems 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

3. 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).

4. 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).

5. 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).

6. As to claim 7, 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).

7. As to claim 8, Schoen discloses 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 (par. 69, lines 21-32);

and a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (Schoen; claim 10, lines 2-5);

where 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 (Schoen: claim 9, lines 4-7),

where at least on 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 Sems. Sems 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

8. As to claims 9 and 10, although the system of Schoen illustrates substantial features of the claim invention, it does not discloses:

A device where 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 (claim 9).

A system where the visual indication of the security mode is provided by a security options screen (claim 10).

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 Sems. Sems discloses:

A device where 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]) (claim 9).

A system where the visual indication of the security mode is provided by a security options screen (to provide on a display a visual indication (e.g., red ribbon) of a security level [red ribbon icon, p. 3, second to the last paragraph]) (claim 10).

Therefore, given the teachings of Sems, 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 of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

9. As to claim 11, Schoen discloses a device where the 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. 30, lines 3- 7), where a visual

indication is provided to the device's user to indicate the updated security mode of operation (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 device's user. 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 Sems. Sems discloses the claim limitation element of the output being configured to comprise a visual indication of the security mode of operation to the device's user (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 security level of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

10. As to claim 12, Schoen discloses a device where a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store (par. 30, lines 3-7).

11. As to claim 13, 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 (par. 30, lines 7-10).

12. As to claim 14, 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 (par. 73, lines 16-23; Schoen; claim 9, lines 4-7).

13. As to claim 15, Schoen discloses a method for use in establishing a security-related mode of operation for computing devices, comprising:

storing a security mode of operation in a policy data store (par. 69, lines 10- 15);

sending the stored security mode of operation to the computing devices over a network (par. 73, lines 16-20);

where the sent security mode of operation places the computing devices into one or more predetermined security-related modes of operation (par. 69, line 13-15).

where at least on 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 Sems. Sems 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

14. As to claim 16, Schoen discloses a method further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store (par. 60, lines 3-5).

15. As to claim 17, Schoen discloses 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 (par. 65, lines 17-21).

16. As to claim 18, Schoen discloses a method further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation (par. 66, lines 11-13; par. 73, lines 16-23).

17. As to claim 20, Schoen discloses a digital signal containing the sent security mode of operation of claim 15 (par. 9, lines 3-6).

18. As to claim 21, Schoen discloses a computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method (Schoen; claim 12, lines 1-3).

19. As to claim 22, Schoen discloses 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 (Schoen: claim 4, lines 1-5; par. 32, lines 3-7);

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 (par. 9, lines 1-6);

Schoen does not expressly teach the claim limitation element of a means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device. 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 Sems. Sems discloses the claim limitation element of a means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

20. Claims 2, 3, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Sems, as applied to claims 1 and 15, and further in view of Wenocur et al. (US Patent Publication No. 2002/0165912 and Wencour hereinafter).

21. As to claims 2, 3, and 19, 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 19).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Sems as introduced by Wencour. Wencour discloses:

A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2) (par. 254, lines 1-13) to provide a secure mode of operation. A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3) (par. 257, lines 1-7) to provide the means to utilize encryption.

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 19) (par. 257, lines 1-7) to provide the means to utilize encryption.

Therefore, given the teachings of Wencour a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Sems by employing the well known features of Federal Information Processing Standard (FIPS) and Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) disclosed above by Wencour, for which secure mode will be enhanced (par. 257, lines 1-7).

22. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Sems, as applied to claims 1 and 5, and further in view of Lord et al. (US Patent No. 7,131,003 and Lord hereinafter).

23. As to claim 23, although the system disclose by Schoen in view of Sems shows substantial features of the claimed invention (discussed in the paragraphs above), It fails to disclose:

A system where 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 (claim 23);

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Sems as introduced by Lord. Lord discloses:

A system where 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 (claim 23) (for purposes of policy (i.e., first security mode data structure) cryptographic operations Load provides FIPS capability [col. 5, lines 5-15] such that modification of Schoen teachings of AES and DES encryption provides enhanced security policy related operations);

Therefore, given the teachings of Lord, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Sems by employing the well known features of FIPS cryptographic operations disclosed above by Lord, for which security policy related operations will be enhanced [col. 5, lines 5-15].

22. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Sem, as applied to claim 1, and further in view of Dutta et al. (US Patent Publication No. 20020186845 and Dutta hereinafter).

24. As to claim 24, although the system of Schoen in view of Sems illustrates substantial features of the claim invention, the combined teaching do not disclose:

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.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schoen in view of Sems as introduced by Dutta. Dutta 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 (to provide the capability to disable security setting through a push message (e.g., disable message) [par. 9]).

Therefore, given the teachings of Dutta, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen in view of Sems by employing the well known feature of using a push message to disable security features in a mobile environment disclosed above by Dutta, for which security policy related operations will be enhanced [par. 9].

Prior Art Made of Record

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Shell et al. (US Patent Publication No. 2005/0190764)

Response to Arguments

Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection. Applicant alleges Schoen is deficient in teaching a visual indication of security level. Examiner contends applicant's deficiency argument is moot on the basis of the teaching of Sems, page 3. Sems teaches the use of a “red ribbon” as a visual indicator to indicate the present security level.

With regards to applicant’s newly added dependent claim 24, Examiner has rejected this claim under the teaching of Schoen in view of Dutta. Dutta specifically teaches a push message (e.g., disable message) to disable a security feature in a mobile environment [par. 9].

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, AYAZ Sheikh can be reached on (571)272-3795. 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

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/065,901	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-2002/0186845	12-2002	Dutta et al.	380/247
*	B	US-2005/0190764	09-2005	Shell et al.	370/389
	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	Sems, Marty, "Verifying Idnetity in a Digital World" August 2000
	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.

Index of Claims	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F 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	01/30/2008	07/18/2008	03/23/2009						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						
	22	✓	✓	✓						
	23		✓	✓						
	24			✓						

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1112	configuration near3 message same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:12
L2	0	l1 and visual near3 indication same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
L3	39	visual near3 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
L4	10	l3 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
L5	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
L6	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
L7	39	visual near5 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17

L8	10	l7 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
L9	603	visual near5 indication and security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
L10	237	l9 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
L11	128	l10 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
L12	4	l10 and push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
L13	3	"20050020244"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
L14	1565	configuration near message and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
L15	3	l14 and visual same setting same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22

L16	2	l14 and security same setting same displayed same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
L17	1739	push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
L18	0	l17 and visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
L19	237	visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
L20	54	l19 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:24
L21	375	visual same security same (setting or mode) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
L22	111	l21 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
L23	111	l22	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25

L24	31	l22 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
L25	25809	security same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
L26	8744981	l25 an(d visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
L27	1195	l25 and (visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
L28	369	l27 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
L29	157	l28 and (security same (mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
L30	87	l29 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:28
L31	225	l28 and (security same (mode or setting or level))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29

L32	135	l31 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
L33	8064	visual same indication same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
L34	1602	l33 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
L35	390	l34 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
L36	200	l35 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
L37	132	l35 and (security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
L38	20	l35 and (security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
L39	2059	(security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33

L40	301	(security same (level or mode or setting)) same visual same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
L41	238	l40 and config$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
L42	128	l40 and (config$9 same (message or instruct$9 or setting)) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:35
L43	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
L44	1082101	l43 and display$9 or visual$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
L45	2	l43 and (display$9 or visual$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
L46	551	(visual$9 same (indicate or indication or indicator) same security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:43
L47	389	l46 and configur$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44

L48	97	l47 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
L49	17	l48 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:46
L50	8093	device same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
L51	2647	l50 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
L52	167	l51 and (visual$5 near (indicator or indication or indicate))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
L53	1054	(security near3 (indicator or indication or indicate) near4 (mode or level or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
L54	48	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
L55	124	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display $9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54

L56	34	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display $9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
L57	192	icon same encrypted same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
L58	119	icon same encrypted same message same user	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
L59	52	l58 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S1	0	"11067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S2	0	"11/067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S3	0	"11071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S4	2	"11/071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S5	1	"20030145214"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:39
S6	2	S4 and unique	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:40
S7	1	S5 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:46
S8	1	("7287282").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S9	1	S8 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S10	0	2005/005098	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S11	1	"2005005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S12	1	"20050005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34

S13	0	"11071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:01
S14	1	"11/071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S15	0	S14 and plurality	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S16	1	S14 and hardware	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S17	0	S14 and (serial same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S18	1	S14 and (image same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S19	1	S14 and (image same software same hardware)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S20	1	S12 and serial$9	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:16
S21	1	"20020010855"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:55
S22	3	"11056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:58
S23	3	"11/056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 17:00
S24	1	"20050004873"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:01
S25	4	"60,444,581"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:03
S26	0	"11067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S27	0	"11.067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S28	1	"11/067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S29	1	S28 and (print near monitor)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:47
S30	2	2003/0014368	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S31	1	S30 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S32	1	"20030014368"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S33	1	S32 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S34	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S35	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42

S36	1	"20030204722"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:43
S37	0	S26 and security	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:44
S38	1	S35 and (security near mode)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:00
S39	1	S36 and (securit$9)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:55
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13
S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$.DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30
S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40

S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46
S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51
S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45
S54	1	S53 and mode	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:46
S55	1	"11056219"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S56	1	"7278155"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S57	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S58	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S59	386	enable same disable same security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19

S60	35	S59 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S61	13	S60 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S62	105	security same mode same (deployed or deploy or deploying) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S63	97	S62 and (enabl$9 or disabl$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S64	30	S63 and security same policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S65	8628	PIM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S66	1073	S65 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S67	2	S66 and moble	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S68	724	S66 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S69	406	S68 and GSM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S70	38	S69 and security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:30
S71	144	message near server same redirected same mobile same received	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S72	130	S71 and gsm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35

S73	79	S72 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S74	103	pull same message same access same scheme	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S75	38	S74 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S76	10	disable same message same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:08
S77	1	11/065901	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:09
S78	68	disable same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S79	5	S78 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S80	886	disable near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13

S81	117	S80 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S82	28	S81 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S83	18	S82 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:14
S84	4	("6219694").pn. or ("7065347").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:23
S85	402	redirection near server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S86	146	S85 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S87	27	S86 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S88	15	S87 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45

S89	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:51
S90	40	(disable near (message or signal or notification) same disabling same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:58
S91	2	S90 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 11:01
S92	15723	(disable near (message or signal or notification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S93	511	S92 and GSM	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S94	8	S93 and security near4 setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S95	57	S93 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:35
S96	1308	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 13:08

3/25/2009 11:35:42 AM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

Search Notes	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F WRIGHT	**Art Unit** 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright
726	1	3/23/2009	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203	1/29/2008	Bryan Wright
Additional search class/subclass 713/168	7/18/2008	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	3/23/2009	Bryan Wright
Additional search class/subclass 380/247	3/23/2009	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	15723	(disable near (message or signal or notification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
L2	511	l1 and GSM	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
L3	8	l2 and security near4 setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
L4	57	l2 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:35
L5	1308	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 13:08
S1	0	"11067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S2	0	"11/067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S3	0	"11071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S4	2	"11/071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S5	1	"20030145214"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:39
S6	2	S4 and unique	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:40
S7	1	S5 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:46

S8	1	("7287282").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S9	1	S8 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S10	0	2005/005098	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S11	1	"2005005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S12	1	"20050005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S13	0	"11071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:01
S14	1	"11/071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S15	0	S14 and plurality	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S16	1	S14 and hardware	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S17	0	S14 and (serial same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S18	1	S14 and (image same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S19	1	S14 and (image same software same hardware)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S20	1	S12 and serial$9	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:16
S21	1	"20020010855"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:55
S22	3	"11056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:58
S23	3	"11/056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 17:00
S24	1	"20050004873"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:01
S25	4	"60,444,581"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:03
S26	0	"11067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S27	0	"11.067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S28	1	"11/067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S29	1	S28 and (print near monitor)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:47

S30	2	2003/0014368	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S31	1	S30 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S32	1	"20030014368"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S33	1	S32 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S34	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S35	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S36	1	"20030204722"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:43
S37	0	S26 and security	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:44
S38	1	S35 and (security near mode)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:00
S39	1	S36 and (securit$9)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:55
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13
S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$. DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30

S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40
S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46
S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51
S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45

S54	1	S53 and mode	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:46
S55	1	"11056219"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S56	1	"7278155"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S57	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S58	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S59	386	enable same disable same security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S60	35	S59 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S61	13	S60 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S62	105	security same mode same (deployed or deploy or deploying) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S63	97	S62 and (enabl$9 or disabl$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S64	30	S63 and security same policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S65	8628	PIM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S66	1073	S65 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S67	2	S66 and moble	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S68	724	S66 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S69	406	S68 and GSM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S70	38	S69 and security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:30

S71	144	message near server same redirected same mobile same received	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S72	130	S71 and gsm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S73	79	S72 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S74	103	pull same message same access same scheme	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S75	38	S74 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S76	10	disable same message same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:08
S77	1	11/065901	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:09
S78	68	disable same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12

S79	5	S78 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S80	886	disable near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S81	117	S80 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S82	28	S81 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S83	18	S82 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:14
S84	4	("6219694").pn. or ("7065347").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:23
S85	402	redirection near server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S86	146	S85 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44

S87	27	S86 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S88	15	S87 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S89	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:51
S90	40	(disable near (message or signal or notification) same disabling same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:58
S91	2	S90 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 11:01

3/23/2009 1:08:39 PM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

FORM PTO-1449 (Modified) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	Atty Docket No.: 555255012798
	Application No.: 11/065,901
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary)	Applicant: Adams et al
	Filed: 2/25/05
(37 CFR 1.98(b))	Group: ~~2131~~ 2431 Bryan Wright

U.S. PATENT DOCUMENTS

Exam. Init.		Patent Number	Issue/Publ Date	Patentee	Class	Sub-class	Filing Date

FOREIGN PATENT OR PUBLISHED FOREIGN PATENT APPLICATION

Exam. Init.		Document Number	Publication Date of Grant	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No

OTHER DOCUMENTS (Including Author, Title, Date**, Relevant pages, Place of Publication***)

/B.W./		Supplementary European Search Report, issued 7/11/07 by European Patent Office, for European Patent App. No. 05714536
/B.W./		S. Gavrila et al, "Assigning and Enforcing Security Policies on Handheld Devices", Canadian Information Technology Security Symposium, 5/17/02, pages 0-7, XP002440113

Examiner /Bryan Wright/	Date Considered 03/23/2009

EXAMINER: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	4158
Examiner	:	Bryan F. Wright

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSIVE AMENDMENT

Dear Sir:

This Amendment is submitted in response to the Office Action issued on March 30, 2009. Please amend the application as indicated and consider the following remarks. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

IN THE CLAIMS

1. (Previously Presented) 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 computing devices over a network;

wherein the security mode of operation places the 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.

2. (Original) The system of claim 1, wherein the secure 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. (Previously Presented) The system of claim 1, further comprising an administrator interface for updating the configuration data related to a plurality of computing devices that is stored in the policy data store and for communicating security modes of operation to the computing devices;

wherein 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;

wherein the policy data store stores IT security policies related to the 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.

7. (Original) The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Previously Presented) 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 secure 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.

9. (Original) The device of claim 8, 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.

10. (Previously Presented) The device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. (Original) The device of claim 10, 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.

12. (Previously Presented) The device of claim 11, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

13. (Original) The device of claim 8, 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.

14. (Original) The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Previously Presented) 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.

16. (Original) The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. (Previously Presented) The method of claim 15, 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.

18. (Previously Presented) The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. (Original) The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. (Original) A digital signal containing the sent security mode of operation of claim 15.

21. (Original) Computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15.

22. (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.

23. (Previously Presented) 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.

24. (Previously Presented) 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.

REMARKS

Claims 1-24 are pending in the instant application and stand rejected. Assignee respectfully traverses the rejections of the pending claims.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 4-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2003/0204722, application of Schoen, et al. (Schoen), in view of "Verifying Identity In A Digital World" by Marty Sems (Sems). Claims 2-3 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of Sems in further view of U.S. Publication No. 2002/0165912, application of Wenocur, et al. (Wenocur). Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Sems in further view of U.S. Patent No. 7,131,003 (Lord). Claim 24 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Sems in further view of U.S. Patent Publication No. 2002/0186845 (Dutta). Assignee respectfully disagrees with the rejections.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. Claim 1 specifically recites that the computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, where the output is configured to comprise a visual indication of the security mode of operation ***of the user device to the user of the device***. This allows a user of the device to see an indication of which specific security mode the device is operating.

In the rejection of claim 1, the office action correctly admits that "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." In rejecting this feature of claim 1, the office action cites to the second to last paragraph of page 3 of Sems. This passage from Sems cited in the office action reads:

> When your friend receives the signed e-mail, her e-mail program should automatically verify your digital signature. Her copy of Outlook Express will apply the same signature algorithm (this time using your public key) and then the same hash algorithm to the message digest to reconstitute the copied message. If this version of the message matches the plaintext (unencoded) message, it will prove that the message was not altered in transit. Your friend will see a red ribbon icon above the message.

It is respectfully submitted that this citation to Sems also does not teach sending an output to a display of a visual indication of the security mode of operation ***of the device*** to the user of the device, as is expressly required by claim 1. The red ribbon identifies that the digital signature of a received e-mail has been verified. However, this indication of whether or not a digital signature on a received e-mail message has been verified is not at all an indication to the user of the device of the security mode of the device. The device could be in any of a number of security modes and still display the red ribbon of Sems showing that a digital signature on an e-mail has been verified. The Sems ribbon is indicative of a fact about the e-mail message. It is not indicative of the security mode status of the device. As admitted in the office action, Schoen does not teach an out being configured to comprise a visual indication of the security mode of operation of the device to the user of the device. Because the Sems red ribbon is also not a visual indication of the security mode of operation of the device to the user of the device, it is respectfully submitted that Sems does not provide a sufficient teaching or suggestion for a *prima facie* case for obviousness. Therefore, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

Independent claims 8, 15, and 22 also were rejected based upon the Schoen and Sems references. Claims 8, 15, and 22 recite subject matter analogous to that of claim 1. Given that claims 8, 15, and 22 recite subject matter analogous to the subject matter of claim 1, and that the subject matter is not disclosed by Schoen and Sems, these claims are allowable for at least the reasons set forth above with respect to claim 1. Therefore, claims 8, 15, and 22 should proceed to issuance.

With reference to claim 18, claim 18 recites the step of receiving an indication that the device has received and entered into the sent security mode of operation. In rejecting claim 18, the office action cites to paragraph 66 and paragraph 73 of Schoen as teaching or suggesting the limitation. Paragraph 63 states that upon receiving a request from a sender to establish a secure connection, the recipient may notify the sender that a secure connection is not possible. An indication that a secure connection is not possible is not an indication that a device has received the sent security mode of operation and has entered into the sent security mode of operation. It is only an indication that a secure connection is not possible. This could be for a variety of reasons including the recipient device not having hardware capable of implementing the secure connection, one of a multiple security protocols that does not permit a secure connection being active, etc. Thus, paragraph 63 does not give an indication of receipt and entrance into a specific sent security mode. Paragraph 73 describes an administrator creating and broadcasting policy certificates. However, these activities also do not indicate whether a device has received or implemented those broadcasted policies. Thus, paragraph 73 also does not teach the feature of claim 18. Because the cited portions of the references do not teach or suggest the feature of claim 18, it is respectfully requested that the § 103 rejection of claim 18 be withdrawn.

It should be noted that assignee has not presented arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to assignee's right to present arguments to all of the dependent claims at any point in the future. In addition, because each of the dependent claims depends from a base claim that is itself allowable, the dependent claims are allowable for at least these reasons and should proceed to issuance.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

Date: June 26, 2009

By:

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point; 901 Lakeside Avenue
Cleveland, OH 44114
(216) 586-3939

Electronic Acknowledgement Receipt

EFS ID:	5596274
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
Title of Invention:	System and method for configuring devices for secure operations
First Named Inventor/Applicant Name:	Neil P. Adams
Correspondence Address:	John V. Biernacki, Esq. JONES DAY North Point 901 Lakeside Avenue Cleveland OH 44114 US 2165863939 -
Filer:	Stephen D. Scanlon/John V. Biernacki
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255012798
Receipt Date:	26-JUN-2009
Filing Date:	25-FEB-2005
Time Stamp:	15:07:11
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	Amendment/Req. Reconsideration-After Non-Final Reject	DOC136.pdf	375079 cdaf0b089fd60bb0eed92f05ffe5bd4df2db235c	no	11
Warnings:					
Information:					
			Total Files Size (in bytes):	375079	

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.

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 11/065,901	Filing Date 02/25/2005	□ 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))							
			TOTAL			TOTAL	

* 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	06/26/2009	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 $52=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	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:
/BRENDA MURPHY/

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

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/065,901		2431	

OC000000037317099

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 89441 on 08/11/2009

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 89441 is:

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

PART 1 - ATTORNEY/APPLICANT COPY

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

89441 7590 11/13/2009

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
11/13/2009	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.** 11/065,901	**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 6/26/2009.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ 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

4)☒ Claim(s) 1-24 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-24 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ 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).

11)□ 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

12)□ 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 _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

FINAL ACTION

1. This action is in response to Amendment filed 6/26/2009. Claims 1-24 are pending.

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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1, 4-18, and 20-22 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 Marty Sems (NPL "Verifying Identity In A Digital World" and Sems hereinafter).

3. As to claims 1, 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 security mode data structure stores a security mode of operation (par. 69, line 13-15);

where the stored security mode of operation is provided to the computing devices over a network (par. 73, lines 16-20);

where the security mode of operation places the computing devices in a predetermined security mode of operation (par. 69, line 13-15);

where at least on 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 Sems. Sems 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

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 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).

8. As to claim 8, Schoen discloses 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 (par. 69, lines 21-32);

and a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (Schoen; claim 10, lines 2-5);

where 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 (Schoen: claim 9, lines 4-7), where at least on 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 Sems.

Sems 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

9. As to claims 9 and 10, although the system of Schoen illustrates substantial features of the claim invention, it does not discloses:

A device where 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 (claim 9).

A system where the visual indication of the security mode is provided by a security options screen (claim 10).

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 Sems. Sems discloses:

A device where 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]) (claim 9).

A system where the visual indication of the security mode is provided by a security options screen (to provide on a display a visual indication (e.g., red ribbon) of a security level [red ribbon icon, p. 3, second to the last paragraph]) (claim 10).

Therefore, given the teachings of Sems, 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 of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

10. As to claim 11, Schoen discloses a device where the 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. 30, lines 3-7), where a visual indication is provided to the device's user to indicate the updated security mode of operation (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 device's user.

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 Sems. Sems discloses the claim limitation element of the output being configured to comprise a visual indication of the security mode of operation to the device's user (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 security level of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

11. As to claim 12, Schoen discloses a device where a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store (par. 30, lines 3-7).

12. As to claim 13, 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 (par. 30, lines 7-10).

13. As to claim 14, 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 (par. 73, lines 16-23; Schoen; claim 9, lines 4-7).

14. As to claim 15, Schoen discloses a method for use in establishing a security- related mode of operation for computing devices, comprising: storing a security mode of operation in a policy data store (par. 69, lines 10- 15); sending the stored security mode of operation to the computing devices over a network (par. 73, lines 16-20); where the sent security mode of operation places the

computing devices into one or more predetermined security-related modes of operation (par. 69, line 13-15). where at least on 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 Sems. Sems 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 (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

15. As to claim 16, Schoen discloses a method further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store (par. 60, lines 3-5).

16. As to claim 17, Schoen discloses 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 (par. 65, lines 17-21).

17. As to claim 18, Schoen discloses a method further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation (par. 66, lines 11-13; par. 73, lines 16-23).

18. As to claim 20, Schoen discloses a digital signal containing the sent security mode of operation of claim 15 (par. 9, lines 3-6).

19. As to claim 21, Schoen discloses a computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method (Schoen; claim 12, lines 1-3).

20. As to claim 22, Schoen discloses 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 (Schoen: claim 4, lines 1-5; par. 32, lines 3-7);

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 (par. 9, lines 1-6).

Schoen does not expressly teach the claim limitation element of a means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device.

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 Sems. Sems discloses the claim limitation element of a means for displaying the security mode of operation to a user of the computing device through a display associated with the computing device (to provide a visual indication (e.g., red ribbon) for display to a device user that is indicative of the determined security-related level [red ribbon icon, p. 3, second to the last paragraph]).

Therefore, given the teachings of Sems, 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 of a message disclosed above by Sems, for which configuring devices for secure operation will be enhanced [red ribbon icon, p. 3, second to the last paragraph].

21. Claims 2, 3, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Sems, as applied to claims 1 and 15, and further in view of Wenocur et al. (US Patent Publication No. 2002/0165912 and Wencour hereinafter).

22. As to claims 2, 3, and 19, 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 19).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Sems as introduced by Wencour. Wencour discloses:

A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2) (par. 254, lines 1-13) to provide a secure mode of operation.

A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3) (par. 257, lines 1-7) to provide the means to utilize encryption.

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 19) (par. 257, lines 1-7) to provide the means to utilize encryption.

Therefore given the teachings of Wencour a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Sems by employing the well known features of Federal Information Processing Standard (FIPS) and Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) disclosed above by Wencour, for which secure mode will be enhanced (par. 257, lines 1-7).

23. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Sems, as applied to claims 1 and 5, and further in view of Lord et al. (US Patent No. 7,131,003 and Lord hereinafter).

24. As to claim 23, although the system disclose by Schoen in view of Sems shows substantial features of the claimed invention (discussed in the paragraphs above), It fails to disclose:

A system where 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 (claim 23).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Sems as introduced by Lord. Lord discloses:

A system where 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 (claim 23) (for purposes of policy (i.e., first security mode data structure) cryptographic operations Load provides FIPS capability [col. 5, lines 5-15] such that modification of Schoen teachings of AES and DES encryption provides enhanced security policy related operations).

Therefore, given the teachings of Lord, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Sems by employing the well known features of FIPS cryptographic operations disclosed above by Lord, for which security policy related operations will be enhanced [col. 5, lines 5-15].

25. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Sem, as applied to claim 1, and further in view of Dutta et al. (US Patent Publication No. 20020186845 and Dutta hereinafter).

26. As to claim 24, although the system of Schoen in view of Sems illustrates substantial features of the claim invention, the combined teaching do not disclose:

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.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schoen in view of Sems as introduced by Dutta. Dutta 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 (to provide the capability to disable security setting through a push message (e.g., disable message) [par. 9]).

Therefore, given the teachings of Dutta, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen in view of Sems by employing the well known feature of using a push message to disable security features in a mobile environment disclosed above by Dutta, for which security policy related operations will be enhanced [par. 9].

Response to Arguments

With regard to applicant’s alleged deficiency on the part of Schoen in view of Sems as it pertains to the claim limitation element of, " …a visual indication of the security mode of operation to the user of the one of the plurality of computing devices”, the Examiner submits that Sems discloses on page 10, a visual indication of the security settings (i.e., mode). The security settings are visually displayed on the users computer screen. The Examiner further submits that Sems security setting depicts the communication security mode.

Additionally, the Examiner respectfully submits that Sems discloses on page 11, a "closed padlock” icon near the bottom of the screen display. The Examiner contends those skilled in the art would construe the "closed padlock” icon disclosed by Sems to visually indicate a specific type of security mode that the user computer has entered into. In this instance the security mode (e.g., setting) would be secure communication.

With regards to applicant's argument alleging deficiency on the part of Schoen as it pertains to the claim limitation element of, "receiving an indication that the device has received and entered into the sent security mode of operation", the Examiner respectfully submits that Schoen disclose in paragraph 81 the following: " …determining whether a secure instant message state change notification has been received. If one has been received, … then analyzed as previously described to indicate whether a change in state should occur". The Examiner respectfully submits that Schoen further discloses, "… then notifies the message processor of any changes in state to effect a new state change". The Examiner contends that Schoen specifically states that a change of state has occurred in the event of a successful verification and that the notification indicates the actual change in state taken place; the "state changes" being associated with the operation security (i.e., setting) state of the device.

Moreover, Sems discloses on page 11, a "closed padlock icon". The Examiner contends the mode determination is representative of the padlock being "open" or "closed". The mode would only change under the required input (i.e., received input). Those skilled in the art would recognize the lock padlock being representative of a secure state and an open padlock as representative of a unsecure state.

Applicant's arguments filed 6/26/2009 have been fully considered but they are not persuasive.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

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, William Korzuch can be reached on (571) 272-7589. 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

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

Index of Claims	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F 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	01/30/2008	07/18/2008	03/23/2009	11/04/2009					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					
	17	✓	✓	✓	✓					
	18	✓	✓	✓	✓					
	19	✓	✓	✓	✓					
	20	✓	✓	✓	✓					
	21	✓	✓	✓	✓					
	22	✓	✓	✓	✓					
	23		✓	✓	✓					
	24			✓	✓					

Search Notes	Application/Control No. 11065901	Applicant(s)/Patent Under Reexamination ADAMS ET AL.
	Examiner BRYAN F WRIGHT	Art Unit 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright
726	1	3/23/2009	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203	1/29/2008	Bryan Wright
Additional search class/subclass 713/168	7/18/2008	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	3/23/2009	Bryan Wright
Additional search class/subclass 380/247	3/23/2009	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1646	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/04 16:42
S1	0	"11067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S2	0	"11/067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S3	0	"11071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S4	2	"11/071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S5	1	"20030145214"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:39
S6	2	S4 and unique	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:40
S7	1	S5 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:46
S8	1	("7287282").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S9	1	S8 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S10	0	2005/005098	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S11	1	"2005005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S12	1	"20050005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S13	0	"11071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:01
S14	1	"11/071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S15	0	S14 and plurality	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S16	1	S14 and hardware	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S17	0	S14 and (serial same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S18	1	S14 and (image same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06

S19	1	S14 and (image same software same hardware)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S20	1	S12 and serial$9	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:16
S21	1	"20020010855"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:55
S22	3	"11056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:58
S23	3	"11/056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 17:00
S24	1	"20050004873"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:01
S25	4	"60,444,581"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:03
S26	0	"11067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S27	0	"11.067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S28	1	"11/067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S29	1	S28 and (print near monitor)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:47
S30	2	2003/0014368	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S31	1	S30 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S32	1	"20030014368"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S33	1	S32 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S34	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S35	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S36	1	"20030204722"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:43
S37	0	S26 and security	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:44
S38	1	S35 and (security near mode)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:00
S39	1	S36 and (securit$9)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:55
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13

S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$.DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30
S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40
S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46

S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51
S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45
S54	1	S53 and mode	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:46
S55	1	"11056219"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S56	1	"7278155"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S57	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S58	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S59	386	enable same disable same security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S60	35	S59 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S61	13	S60 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S62	105	security same mode same (deployed or deploy or deploying) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S63	97	S62 and (enabl$9 or disabl $9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25

S64	30	S63 and security same policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S65	8628	PIM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S66	1073	S65 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S67	2	S66 and moble	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S68	724	S66 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S69	406	S68 and GSM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S70	38	S69 and security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:30
S71	144	message near server same redirected same mobile same received	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S72	130	S71 and gsm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S73	79	S72 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S74	103	pull same message same access same scheme	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S75	38	S74 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41

S76	10	disable same message same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:08
S77	1	11/065901	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:09
S78	68	disable same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S79	5	S78 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S80	886	disable near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S81	117	S80 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S82	28	S81 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S83	18	S82 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:14
S84	4	("6219694").pn. or ("7065347").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:23

S85	402	redirection near server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S86	146	S85 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S87	27	S86 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S88	15	S87 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S89	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:51
S90	40	(disable near (message or signal or notification) same disabling same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:58
S91	2	S90 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 11:01
S92	15723	(disable near (message or signal or notification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S93	511	S92 and GSM	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33

S94	8	S93 and security near4 setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S95	57	S93 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:35
S96	1308	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 13:08
S97	1112	configuration near3 message same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:12
S98	0	S97 and visual near3 indication same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S99	39	visual near3 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S100	10	S99 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S101	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
S102	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15

S103	39	visual near5 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S104	10	S103 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S105	603	visual near5 indication and security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S106	237	S105 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S107	128	S106 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S108	4	S106 and push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S109	3	"20050020244"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S110	1565	configuration near message and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S111	3	S110 and visual same setting same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22

S112	2	S110 and security same setting same displayed same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
S113	1739	push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S114	0	S113 and visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S115	237	visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S116	54	S115 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:24
S117	375	visual same security same (setting or mode) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S118	111	S117 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S119	111	S118	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S120	31	S118 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25

S121	25809	security same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S122	8744981	S121 an(d visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S123	1195	S121 and (visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S124	369	S123 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S125	157	S124 and (security same (mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S126	87	S125 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:28
S127	225	S124 and (security same (mode or setting or level))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S128	135	S127 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S129	8064	visual same indication same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32

S130	1602	S129 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S131	390	S130 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S132	200	S131 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S133	132	S131 and (security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S134	20	S131 and (security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S135	2059	(security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S136	301	(security same (level or mode or setting)) same visual same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S137	238	S136 and config$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S138	128	S136 and (config$9 same (message or instruct$9 or setting)) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:35

S139	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S140	1082101	S139 and display$9 or visual$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S141	2	S139 and (display$9 or visual$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S142	551	(visual$9 same (indicate or indication or indicator) same security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:43
S143	389	S142 and configur$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S144	97	S143 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S145	17	S144 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:46
S146	8093	device same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S147	2647	S146 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48

S148	167	S147 and (visual$5 near (indicator or indication or indicate))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S149	1054	(security near3 (indicator or indication or indicate) near4 (mode or level or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S150	48	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S151	124	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S152	34	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S153	192	icon same encrypted same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S154	119	icon same encrypted same message same user	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S155	52	S154 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S156	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 10:20

S157	2	"20030204722"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/30 14:29
S158	1	"10592339"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/31 16:48
S159	2	("20030204722")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/04 14:11

11/4/2009 4:45:00 PM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	4158
Examiner	:	Bryan F. Wright

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Dear Sir:

Please consider the following remarks. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

IN THE CLAIMS

1. (Currently Amended) 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 computing devices over a network;

wherein the security mode of operation places the 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 security algorithms.

2. (Currently Amended) The system of claim 1, wherein the ~~secure~~ 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. (Previously Presented) The system of claim 1, further comprising an administrator interface for updating the configuration data related to a plurality of computing devices that is stored in the policy data store and for communicating security modes of operation to the computing devices;

wherein 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;

wherein the policy data store stores IT security policies related to the 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.

7. (Original) The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Currently Amended) 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 ~~secure~~ 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 security algorithms.

9. (Original) The device of claim 8, 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.

10. (Previously Presented) The device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. (Original) The device of claim 10, 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.

12. (Previously Presented) The device of claim 11, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

13. (Original) The device of claim 8, 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.

14. (Original) The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Currently Amended) 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 security algorithms.

16. (Original) The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. (Previously Presented) The method of claim 15, 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.

18. (Previously Presented) The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. (Original) The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. (Original) A digital signal containing the sent security mode of operation of claim 15.

21. (Original) Computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 15.

22. (Currently Amended) 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 security algorithms.

23. (Previously Presented) 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.

24. (Previously Presented) 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.

REMARKS

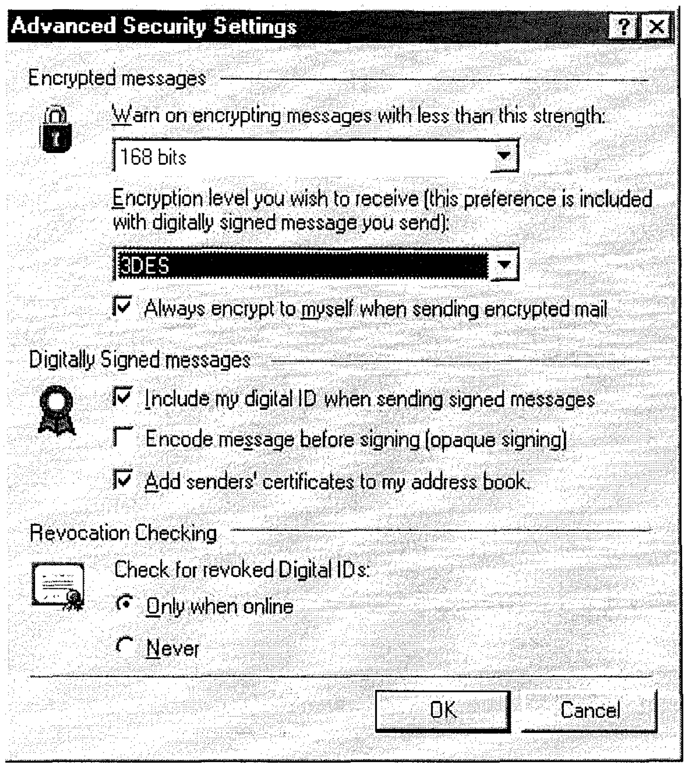
Claims 1-24 are pending in the instant application and stand rejected. Assignee respectfully traverses the rejections of the pending claims.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 4-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2003/0204722, application of Schoen, et al. (Schoen), in view of "Verifying Identity In A Digital World" by Marty Sems (Sems). Claims 2-3 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of Sems in further view of U.S. Publication No. 2002/0165912, application of Wenocur, et al. (Wenocur). Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Sems in further view of U.S. Patent No. 7,131,003 (Lord). Claim 24 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Sems in further view of U.S. Patent Publication No. 2002/0186845 (Dutta). Assignee respectfully disagrees with the rejections.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. Claim 1 specifically recites that the computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, where the output is configured to comprise ***a visual indication of the security mode of operation of the user device to the user of the device.*** This allows a user of the device to see an indication of which specific security mode the device is operating. Additionally, claim 1 has been amended to require that the security mode of operation forces use of one or more security algorithms. Support for this subject matter is found in assignee's specification, such as in lines 17-22 on page 11.

Page 18 of the current office action maintains that Sems discloses the following limitation of claim 1: "a visual indication of the security mode of operation to the user of the one of the plurality of computing devices." More specifically, the office action maintains that the figures on pages 10 and 11 of Sems discloses this limitation of claim 1. The figure on page 10 is as follows:



Advanced Security Settings

Encrypted messages

Warn on encrypting messages with less than this strength:

168 bits

Encryption level you wish to receive (this preference is included with digitally signed message you send):

3DES

☑ Always encrypt to myself when sending encrypted mail

Digitally Signed messages

☑ Include my digital ID when sending signed messages

□ Encode message before signing (opaque signing)

☑ Add senders' certificates to my address book.

Revocation Checking

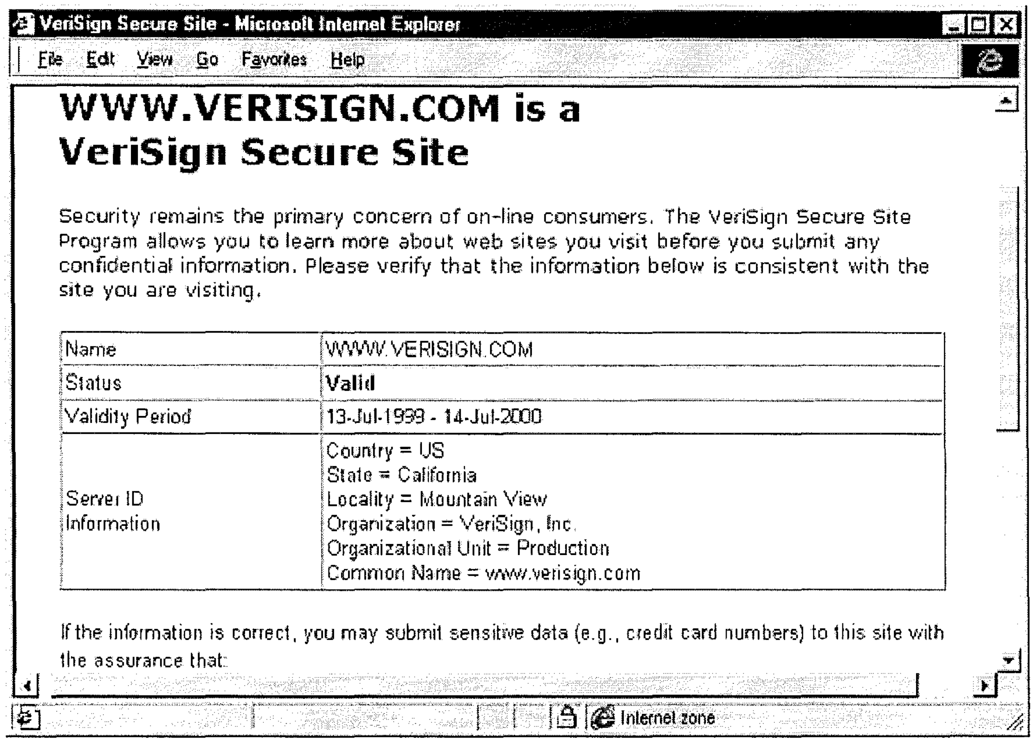
Check for revoked Digital IDs:

● Only when online

○ Never

As shown by the figure above, all of the settings are established by the user, which is the antithesis of what the security mode of operation in claim 1 is to accomplish. In other words, the settings in this figure from Sems are manipulable by the device's user, and not by the specific security mode of operation which in claim 1 is required to have been provided to a computing device over a network.

Similarly, the figure on page 11 of Sems does not disclose the aforementioned limitation of claim 1. The figure on page 11 of Sems is as follows:


VeriSign Secure Site - Microsoft Internet Explorer
File Edit View Go Favorites Help
Internet zone

WWW.VERISIGN.COM is a VeriSign Secure Site

Security remains the primary concern of on-line consumers. The VeriSign Secure Site Program allows you to learn more about web sites you visit before you submit any confidential information. Please verify that the information below is consistent with the site you are visiting.

Name	WWW.VERISIGN.COM
Status	**Valid**
Validity Period	13-Jul-1999 - 14-Jul-2000

Server ID Information	Country = US
	State = California
	Locality = Mountain View
	Organization = VeriSign, Inc.
	Organizational Unit = Production
	Common Name = www.verisign.com

If the information is correct, you may submit sensitive data (e.g., credit card numbers) to this site with the assurance that:

As noted on page 11 of Sems, there is a "closed padlock icon near the bottom, which indicates a secure connection." However, the closed padlock is not a visual indication of a security mode of operation which forces use of one or more security algorithms as required by claim 1. Instead, the figure above from Sems merely indicates that a secure connection has been established – not that the device is constrained to using only certain security algorithms in its operations. Because of such differences between the cited references and the subject matter of claim 1, it is respectfully submitted that the references do not provide a sufficient teaching or suggestion for a prima facie case for obviousness. Therefore, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

Independent claims 8, 15, and 22 also were rejected based upon the Schoen and Sems references. Claims 8, 15, and 22 have been amended to recite subject matter analogous to that of claim 1. Given that claims 8, 15, and 22 recite subject matter analogous to the subject matter of claim 1, and that the subject matter is not disclosed by Schoen and Sems, these claims are allowable for at least the reasons set forth above with respect to claim 1. Therefore, claims 8, 15, and 22 should proceed to issuance.

It should be noted that assignee has not presented arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to assignee's right to present arguments to all of the dependent claims at any point in the future. In addition, because each of the dependent claims depends from a base claim that is itself allowable, the dependent claims are allowable for at least these reasons and should proceed to issuance.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

Date: January 12, 2010

By:

John W. Biernacki
Reg. No. 40,511
JONES DAY
North Point; 901 Lakeside Avenue
Cleveland, OH 44114
(216) 586-3939

Electronic Acknowledgement Receipt

EFS ID:	6793484
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
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/John V. Biernacki
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255012798
Receipt Date:	12-JAN-2010
Filing Date:	25-FEB-2005
Time Stamp:	14:16:43
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	Amendment After Final	DOC002.pdf	518110 a1726e9bb64a5319f2f0211f2d5e0ae9e6c48f21	no	12

Warnings:

Information:

Total Files Size (in bytes):	518110

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.

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 11/065,901	Filing Date 02/25/2005	□ 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	01/12/2010	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 $52=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	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:
/PATSY ZIMMERMAN/

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.

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	4158
Examiner	:	Bryan F. Wright

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Dear Sir:

Please consider the following remarks. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

DO NOT ENTER: /B.W./

01/28/2010

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

89441 7590 02/09/2010

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
02/09/2010	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

PTOL-90A (Rev. 04/07)

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *11/065,901*	**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 --

THE REPLY FILED 12 January 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.

b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) □ They raise the issue of new matter (see NOTE below);
(c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) □ They present additional claims without canceling a corresponding number of finally rejected claims.
NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. □ Applicant's reply has overcome the following rejection(s): _____.

6. □ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) □ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: *1-24*.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. □ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. □ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Note.

12. □ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. □ Other: _____.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Syed Zia/
Primary Examiner, Art Unit 2431

Note: The Examiner respectfully submits applicant's amended claims presented on 1/12/2010 include subject matter that is narrower in scope than previously submitted claims and rasies new issues that will require more consideration. Therefore a new search will be required.

With regards to applicant's remarks concerning the setting of security settings, the Examiner contends the applicant states on page 11 of applicant's specification that an interface exist for a IT professonial (e.g., user) to click on a checkbox to designate security settings. The Examiner respectfully submits that prior art reference Sems teaches such an interface. The Examiner contends that Sems teaches an interface for setting (e.g., configuring the security settings). Refer to page 10 and 11 of Sems.

With regards to applicant's remark pertaining to security status indication, the Examiner contends Sem's disclosure of a "padlock" symobol is representative of the security as it pertains to communication. A close "padlock" symbol has one security meaning as it pertains to communication, and an open "padlock" padlock has another security meaning as it pertains to communication.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	11065901	Filing Date	2005-02-25	Docket Number (if applicable)	555255-012798	Art Unit	2431
First Named Inventor	Neil P. Adams			Examiner Name	Bryan F. Wright		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

□ Consider the arguments in the Appeal Brief or Reply Brief previously filed on ____________

☒ Other Response filed on January 12, 2010

□ Enclosed

□ Amendment/Reply

□ Information Disclosure Statement (IDS)

□ Affidavit(s)/ Declaration(s)

□ Other ____________

MISCELLANEOUS

□ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months ________
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

□ Other ____________

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 501432

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

□ Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Matthew W. Johnson/	Date (YYYY-MM-DD)	2010-03-11
Name	Matthew W. Johnson	Registration Number	59108

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.

Electronic Patent Application Fee Transmittal

Application Number:	11065901
Filing Date:	25-Feb-2005
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:	555255012798

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:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	130	130

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	810	810
	Total in USD ($)			**940**

Electronic Acknowledgement Receipt

EFS ID:	7189192
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
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:	555255012798
Receipt Date:	11-MAR-2010
Filing Date:	25-FEB-2005
Time Stamp:	14:24:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$940
RAM confirmation Number	543
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 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	012798_ext.pdf	58043 273f24d947e3cd7a5695ae2b4b86f16e106cf8ce	no	1
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	RCE_new_MJ.pdf	697477 1e9a9470692dc494a1f3c4ef30d3f90a46ff4a69	no	3
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32165 e0c92694b60fbffbfe386fd782fc25952733dc9d	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	787685	

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.

PTO/SB/22 (12-08)
Approved for use through 01/31/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE
Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)
FY 2009

(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)

Docket Number (Optional) 555255-012798

Application Number 11/065,901

Filed February 25, 2005

For SYSTEM AND METHOD FOR CONFIGURING DEVICES FOR SECURE OPERATIONS

Art Unit 2431

Examiner Bryan F. Wright

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	
☑ One month (37 CFR 1.17(a)(1))	$130	$65	$ 130.00
□ Two months (37 CFR 1.17(a)(2))	$490	$245	$
□ Three months (37 CFR 1.17(a)(3))	$1110	$555	$
□ Four months (37 CFR 1.17(a)(4))	$1730	$865	$
□ Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

□ Applicant claims small entity status. See 37 CFR 1.27.

□ A check in the amount of the fee is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-1432.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the
□ applicant/inventor.
□ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).
☑ attorney or agent of record. Registration Number 59,108
□ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 ______

/Matthew W. Johnson
Signature

March 11, 2010
Date

Matthew W. Johnson
Typed or printed name

(412) 394-9524
Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

□ Total of ______ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

89441 7590 06/24/2010
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
06/24/2010	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.** 11/065,901	**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 *12 January 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ 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

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ 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).

11)□ 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

12)□ 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 _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/12/2010 has been entered. Claims 1, 2, 8, 15 and 22 are amended. Claims 1-24 are pending.

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.

2. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Currently, claim 21 is drawn to a computer product in a computer readable media. The term “media” however under the broadest interpretation includes a transitory signal for which the office considers to be non-statutory subject matter. As such the applicant is advised to include either in the claim language or in the specification subject matter reciting that the media does not include a signal.

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.

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.

1. Claims 1, 4-18, and 20-22 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).

2. As to claims 1, 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 security mode data structure stores a security mode of operation (par. 69, line 13-15); where the stored security mode of operation is provided

to the computing devices over a network (par. 73, lines 16-20); where the security mode of operation places the computing devices in a predetermined security mode of operation (par. 69, line 13-15); where at least on 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, wherein the security mode of operation forces use of one or more security algorithms.
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 security algorithms (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].

3. 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).

4. 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).

5. 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).

6. As to claim 7, 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).

7. As to claim 8, Schoen discloses 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 (par. 69, lines 21-32); and a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (Schoen; claim 10, lines 2-5); where 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 (Schoen: claim 9, lines 4-7), where at least on 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, wherein the security mode of operation forces use of one or more security algorithms.

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 security algorithms (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].

8. As to claims 9 and 10, although the system of Schoen illustrates substantial features of the claim invention, it does not discloses: A device where 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 (claim 9).

A system where the visual indication of the security mode is provided by a security options screen (claim 10). 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. Phillipss discloses:

A device where 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 (to provide a visual indication for display to a device user that is indicative of the determined security-related level [par. 96) (claim 9).

A system where the visual indication of the security mode is provided by a security options screen (to provide on a display a visual indication of a security level [par. 96]) (claim 10).

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 of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

9. As to claim 11, Schoen discloses a device where the 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. 30, lines 3- 7), where a visual indication is provided to the device's user to indicate the updated security mode of operation (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 device's user.

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 device's user (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 security level of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

10. As to claim 12, Schoen discloses a device where a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store (par. 30, lines 3-7).

11. As to claim 13, 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 (par. 30, lines 7-10).

12. As to claim 14, 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 (par. 73, lines 16-23; Schoen; claim 9, lines 4-7).

13. As to claim 15, Schoen discloses a method for use in establishing a security-related mode of operation for computing devices, comprising: storing a security mode of operation in a policy data store (par. 69, lines 10- 15); sending the stored security mode of operation to the computing devices over a network (par. 73, lines 16-20); where the sent security mode of operation places the computing devices into one or more predetermined security-related modes of operation (par. 69, line 13-15). where at least

on 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, wherein the security mode of operation forces use of one or more security algorithms. 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 security algorithms (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 of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

14. As to claim 16, Schoen discloses a method further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store (par. 60, lines 3-5).

15. As to claim 17, Schoen discloses 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 (par. 65, lines 17-21).

16. As to claim 18, Schoen discloses a method further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation (par. 66, lines 11-13; par. 73, lines 16-23).

17. As to claim 20, Schoen discloses a digital signal containing the sent security mode of operation of claim 15 (par. 9, lines 3-6).

18. As to claim 21, Schoen discloses a computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method (Schoen; claim 12, lines 1-3).

19. As to claim 22, Schoen discloses 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 (Schoen: claim 4, lines 1-5; par. 32, lines 3-7); 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 (par. 9, lines 1-6).

Schoen does not expressly teach the claim limitation element of a 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 security algorithms. 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 a 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 security algorithms (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 of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

20. Claims 2, 3, and 19 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).

21. As to claims 2, 3, and 19, 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 19). However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Phillips as introduced by Wencour. Wencour discloses:

A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2) (par. 254, lines 1-13) to provide a secure mode of operation. A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3) (par. 257, lines 1-7) to provide the means to utilize encryption. 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 19) (par. 257, lines 1-7) to provide the means to utilize encryption. Therefore given the teachings of Wencour a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Phillips by employing the well known features of Federal Information Processing Standard (FIPS) and Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) disclosed above by Wencour, for which secure mode will be enhanced (par. 257, lines 1-7).

22. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Phillips, as applied to claims 1 and 5, and further in view of Lord et al. (US Patent No. 7,131,003 and Lord hereinafter).

23. As to claim 23, although the system disclose by Schoen in view of Phillips shows substantial features of the claimed invention (discussed in the paragraphs above), It fails to disclose: A system where 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 (claim 23). However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Phillips as

introduced by Lord. Lord discloses: A system where 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 (claim 23) (for purposes of policy (i.e., first security mode data structure) cryptographic operations Load provides FIPS capability [col. 5, lines 5-15] such that modification of Schoen teachings of AES and DES encryption provides enhanced security policy related operations). Therefore, given the teachings of Lord, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Phillips by employing the well known features of FIPS cryptographic operations disclosed above by Lord, for which security policy related operations will be enhanced [col. 5, lines 5-15]. .

24. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Phillips, as applied to claim 1, and further in view of Dutta et al. (US Patent Publication No. 20020186845 and Dutta hereinafter).

25. As to claim 24, although the system of Schoen in view of Phillips illustrates substantial features of the claim invention, the combined teaching do not disclose: 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. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schoen in view of Phillips as introduced by Dutta. Dutta 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 (to provide the capability to disable security setting through a push message (e.g., disable message) [par. 9]). Therefore, given the teachings of Dutta, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen in view of Phillips by employing the well known feature of using a push message to disable security features in a mobile environment disclosed above by Dutta, for which security policy related operations will be enhanced [par. 9].

Response to Amendment

Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

With regard to applicant's claim limitation element of, " ...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 security algorithms", the Examiner submits that Phillips discloses in paragraph 96, a visual indication of the security settings (i.e., mode). The security settings are visually displayed to the users.

The Examiner further submits that Phillips security setting depicts a particular security mode.

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, William Korzuch can be reached on (571) 272-7589. 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
/Syed Zia/
Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/065,901	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-2005/0183138	08-2005	Phillips et al.	726/011
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1646	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/04 16:42
S1	0	"11067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S2	0	"11/067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S3	0	"11071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S4	2	"11/071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S5	1	"20030145214"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:39
S6	2	S4 and unique	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:40
S7	1	S5 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:46
S8	1	("7287282").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S9	1	S8 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S10	0	2005/005098	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S11	1	"2005005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S12	1	"20050005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S13	0	"11071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:01
S14	1	"11/071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S15	0	S14 and plurality	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S16	1	S14 and hardware	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S17	0	S14 and (serial same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S18	1	S14 and (image same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06

S19	1	S14 and (image same software same hardware)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S20	1	S12 and serial$9	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:16
S21	1	"20020010855"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:55
S22	3	"11056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:58
S23	3	"11/056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 17:00
S24	1	"20050004873"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:01
S25	4	"60,444,581"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:03
S26	0	"11067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S27	0	"11.067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S28	1	"11/067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S29	1	S28 and (print near monitor)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:47
S30	2	2003/0014368	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S31	1	S30 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S32	1	"20030014368"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S33	1	S32 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S34	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S35	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S36	1	"20030204722"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:43
S37	0	S26 and security	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:44
S38	1	S35 and (security near mode)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:00
S39	1	S36 and (securit$9)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:55
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13

S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$.DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30
S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40
S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46

S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51
S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45
S54	1	S53 and mode	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:46
S55	1	"11056219"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S56	1	"7278155"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S57	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S58	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S59	386	enable same disable same security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S60	35	S59 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S61	13	S60 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S62	105	security same mode same (deployed or deploy or deploying) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S63	97	S62 and (enabl$9 or disabl$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25

S64	30	S63 and security same policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S65	8628	PIM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S66	1073	S65 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S67	2	S66 and moble	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S68	724	S66 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S69	406	S68 and GSM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S70	38	S69 and security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:30
S71	144	message near server same redirected same mobile same received	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S72	130	S71 and gsm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S73	79	S72 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S74	103	pull same message same access same scheme	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S75	38	S74 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41

S76	10	disable same message same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:08
S77	1	11/065901	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:09
S78	68	disable same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S79	5	S78 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S80	886	disable near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S81	117	S80 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S82	28	S81 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S83	18	S82 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:14
S84	4	("6219694").pn. or ("7065347").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:23

S85	402	redirection near server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S86	146	S85 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S87	27	S86 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S88	15	S87 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S89	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:51
S90	40	(disable near (message or signal or notification) same disabling same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:58
S91	2	S90 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 11:01
S92	15723	(disable near (message or signal or notification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S93	511	S92 and GSM	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33

S94	8	S93 and security near4 setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S95	57	S93 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:35
S96	1308	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 13:08
S97	1112	configuration near3 message same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:12
S98	0	S97 and visual near3 indication same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S99	39	visual near3 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S100	10	S99 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S101	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
S102	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15

S103	39	visual near5 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S104	10	S103 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S105	603	visual near5 indication and security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S106	237	S105 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S107	128	S106 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S108	4	S106 and push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S109	3	"20050020244"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S110	1565	configuration near message and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S111	3	S110 and visual same setting same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22

S112	2	S110 and security same setting same displayed same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
S113	1739	push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S114	0	S113 and visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S115	237	visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S116	54	S115 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:24
S117	375	visual same security same (setting or mode) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S118	111	S117 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S119	111	S118	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S120	31	S118 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25

S121	25809	security same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S122	8744981	S121 an(d visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S123	1195	S121 and (visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S124	369	S123 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S125	157	S124 and (security same (mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S126	87	S125 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:28
S127	225	S124 and (security same (mode or setting or level))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S128	135	S127 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S129	8064	visual same indication same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32

S130	1602	S129 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S131	390	S130 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S132	200	S131 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S133	132	S131 and (security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S134	20	S131 and (security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S135	2059	(security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S136	301	(security same (level or mode or setting)) same visual same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S137	238	S136 and config$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S138	128	S136 and (config$9 same (message or instruct$9 or setting)) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:35

S139	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S140	1082101	S139 and display$9 or visual$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S141	2	S139 and (display$9 or visual$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S142	551	(visual$9 same (indicate or indication or indicator) same security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:43
S143	389	S142 and configur$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S144	97	S143 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S145	17	S144 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:46
S146	8093	device same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S147	2647	S146 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48

S148	167	S147 and (visual$5 near (indicator or indication or indicate))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S149	1054	(security near3 (indicator or indication or indicate) near4 (mode or level or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S150	48	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S151	124	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S152	34	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S153	192	icon same encrypted same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S154	119	icon same encrypted same message same user	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S155	52	S154 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S156	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 10:20

S157	2	"20030204722"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/30 14:29
S158	1	"10592339"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/31 16:48
S159	2	("20030204722")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/04 14:11

11/4/2009 4:53:48 PM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

Search Notes	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F WRIGHT	**Art Unit** 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright
726	1	3/23/2009	Bryan Wright
726	1	6/19/2010	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203	1/29/2008	Bryan Wright
Additional search class/subclass 713/168	7/18/2008	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	3/23/2009	Bryan Wright
Additional search class/subclass 380/247	3/23/2009	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	6/19/2010	Bryan Wright
Additional search class/subclass 380/247, 726/11	6/19/2010	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Index of Claims	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F 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	01/30/2008	07/18/2008	03/23/2009	11/04/2009	06/19/2010				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	✓				
	6	✓	✓	✓	✓	✓				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	✓	✓	✓				
	16	✓	✓	✓	✓	✓				
	17	✓	✓	✓	✓	✓				
	18	✓	✓	✓	✓	✓				
	19	✓	✓	✓	✓	✓				
	20	✓	✓	✓	✓	✓				
	21	✓	✓	✓	✓	✓				
	22	✓	✓	✓	✓	✓				
	23		✓	✓	✓	✓				
	24			✓	✓	✓				

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	2431
Examiner	:	Bryan F. Wright

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSIVE AMENDMENT

Dear Sir:

This responsive amendment is filed in response to the non-final Office action dated June 24, 2010. Please amend the above-identified application as follows and consider the remarks contained herein. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

IN THE CLAIMS

1. (Currently Amended) 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 computing devices over a network;

wherein the security mode of operation places the 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 ~~security algorithms~~ cryptographic algorithms.

2. (Previously Presented) 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. (Previously Presented) The system of claim 1, further comprising an administrator interface for updating the configuration data related to a plurality of computing devices that is stored in the policy data store and for communicating security modes of operation to the computing devices;

wherein 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;

wherein the policy data store stores IT security policies related to the 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.

7. (Original) The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Currently Amended) 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 ~~security algorithms~~cryptographic algorithms.

9. (Original) The device of claim 8, 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.

10. (Previously Presented) The device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. (Original) The device of claim 10, 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.

12. (Previously Presented) The device of claim 11, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

13. (Original) The device of claim 8, 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.

14. (Original) The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Currently Amended) 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 ~~security algorithms~~cryptographic algorithms.

16. (Original) The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. (Previously Presented) The method of claim 15, 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.

18. (Previously Presented) The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. (Original) The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. (Original) A digital signal containing the sent security mode of operation of claim 15.

21. (Currently Amended) 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 15.

22. (Currently Amended) 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 ~~security algorithms~~cryptographic algorithms.

23. (Previously Presented) 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.

24. (Previously Presented) 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.

REMARKS

Claims 1-24 are pending in the instant application and stand rejected. Assignee respectfully traverses the rejections of the pending claims.

Claim Rejections – 35 U.S.C. § 101

Claim 21 is rejected under 35 U.S.C. § 101as being directed to non-statutory subject matter. Claim 21 is amended to recite computer software stored on one or more non-transitory computer readable media. In light of the amendment, it is respectfully requested that the § 101 rejection of claim 21 be withdrawn.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 4-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2003/0204722, application of Schoen, et al. (Schoen), in view of U.S. Publication No. 2005/0183138, application of Philips et al. (Philips). Claims 2-3 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of Philips in further view of U.S. Publication No. 2002/0165912, application of Wenocur, et al. (Wenocur). Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Philips in further view of U.S. Patent No. 7,131,003 (Lord). Claim 24 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Philips in further view of U.S. Patent Publication No. 2002/0186845 (Dutta). Assignee respectfully disagrees with the rejections.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. Claim 1 specifically recites that the computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, where the output is configured to comprise a visual indication of the security mode of operation of the user device to the user of the device. This allows a user of the device to see an indication of which specific security mode the device is operating. Additionally, claim 1 has been amended to require that the security mode of operation forces use of one or more cryptographic algorithms. Support for this subject matter is found in the specification, such as in lines 17-22 on page 11.

It is respectfully submitted that cited references, individually or in combination, do not disclose the limitations of claim 1. In rejecting claim 1, the Office cites to Schoen and Philips. Admitting Schoen does not teach 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 security algorithms, the Office cites to paragraph [0096] of Philips as disclosing such a feature.

> [0096] Status indicators 910-916 are included to provide a visual indication of the network security module's current status. Status indicators, as previously discusses, are for informational purposes only. They provide optional visual clues to the computer user as to the protective security measures implemented by the network security module 304. Each indicator corresponds to a particular security status. For example, status indicator 910 may correspond to a security level of red, meaning a total lock-down of network activities, and is illuminated in red when the network security module 304 is implementing a total lock-down. Status indicator 912 may correspond to a security level of yellow, i.e., a partial lock-down of network activities, and be illuminated in yellow when the network security module 304 is implementing the partial lock-down. Similarly, status indicator 914 may correspond to the security level green, i.e., free network access, and is illuminated in green when the network security module 304 is permitting unrestricted network access. Status indicator 916 may correspond to the enabled/disabled status of the network security module 304, such that the status indicator is illuminated, perhaps as with a flashing red light, when the network security module is disabled.

However, the cited portion of Philips merely discloses a group of status indicators that provide a visual indication of the network security module's current status, such as a total lock-down of network activities, a partial lock-down of network activities, unrestricted network access, or the disabling of the network security module. However, these statuses are not representative of the cryptographic algorithms required by claim 1. The group of status indicators identify a user's freedom to transmit information on the network but offer no indication of a required cryptographic algorithm that must be used for those transmissions. In fact, the cited portion of Philips never discloses using cryptographic algorithms, let alone forcing use of cryptographic algorithms in a security mode of operation as recited by claim 1. Because the cited references fail to disclose the limitations of claim 1, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

Independent claims 8, 15, 22 are amended to recite similar features as claim 1. These claims are allowable for at least the same reasons as offered for claim 1.

Moreover, the Office fails to make a prima facie unpatentability case against certain dependent claims. For example, the Office cites Schoen, Philips and Wenocur in rejecting claim 3. Specifically, the Office cites to paragraph [0257] of Wenocur as disclosing the FIPS mode of operation includes forcing use of AES or 3DES as recited by claim 3. The cited portion of Wenocur states:

> [0257] The SHA1 digest function shown above ***can be replaced with any cryptographically secure compression or hash or digest function including but not limited to*** MD2, MD4, MD5, RIPE160, SHA-256, SHA-384, SHA-512, DES-CBC-MAC, 3DES-CBC-MAC, IDEA-CBC-MAC, AES-CBC-MAC, DES-MDC, and DES-MDC2. (emphasis added)

At best, Wenocur discloses as an option to use AES or 3DES to replace the SHA1 digest function. Other cryptographic functions, such as MD2, MD4, MD5, RIPE160, SHA-256, SHA-384, SHA-512, can also be used. Thus, it never discloses the FIPS mode of operation forcing use of AES or 3DES as required by claim 3. Because the cited references never disclose the limitations of claim 3, it is respectfully requested that the § 103 rejection of claim 3 be withdrawn.

Dependent claim 19 recites similar subject matter as claim 3 and stands rejected by the Office for similar reasons. Thus, claim 19 is allowable for at least similar reasons as offered for claim 3.

It should be noted that assignee has not presented arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to assignee's right to present arguments to all of the dependent claims at any point in the future. In addition, because each of the dependent claims depends from a base claim that is itself allowable, the dependent claims are allowable for at least these reasons and should proceed to issuance.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

Date: September 21, 2010

Matthew W. Johnson

Matthew W. Johnson
Reg. No. 59,108
Jones Day
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(412) 394-9524

Electronic Acknowledgement Receipt

EFS ID:	8460743
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
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:	555255012798
Receipt Date:	21-SEP-2010
Filing Date:	25-FEB-2005
Time Stamp:	11:43:24
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	Amendment/Req. Reconsideration-After Non-Final Reject	012798_amend.pdf	618162 6806b9e871c839e1582d92b0cb28f89ef39213f4	no	12

Warnings:

Information:

Total Files Size (in bytes):	618162

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.

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 11/065,901	Filing Date 02/25/2005	□ 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	09/21/2010	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	** 25	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	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:
/Theresa Dawkins/

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 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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

89441 7590 01/24/2011

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
01/24/2011	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.** 11/065,901	**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 *21 September 2010*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ 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

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ 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).

11)□ 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

12)□ 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 *1/26/2009*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed 9/21/2010. Claim 1 and 22 are amended. Claims 1-24 are pending.

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, 4-18, and 20-22 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).

3. As to claims 1, 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 security mode data structure stores a security mode of operation (par. 69, line 13-15); where the stored security mode of operation is provided

to the computing devices over a network (par. 73, lines 16-20); where the security mode of operation places the computing devices in a predetermined security mode of operation (par. 69, line 13-15); where at least on 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, wherein the security mode of operation forces use of one or more security algorithms. 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].

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 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).

8. As to claim 8, Schoen discloses 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 (par. 69, lines 21-32); and a processor communicatively coupled to the communication interface, wherein the processor is configured to execute processing instructions (Schoen; claim 10, lines 2-5); where 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 (Schoen: claim 9, lines 4-7), where at least on 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, wherein the security mode of operation forces use of one or more cryptographic algorithm. 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 security algorithms (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].

9. As to claims 9 and 10, although the system of Schoen illustrates substantial features of the claim invention, it does not discloses: A device where 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 (claim 9). A system where the visual indication of the security mode is provided by a security options screen (claim 10). 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. Phillipss discloses: A device where 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 (to provide a visual indication for display to a device user that is indicative of the determined security-related level [par. 96) (claim 9). A system where the visual indication of the security mode is provided by a security options screen (to provide on a display a visual indication of a security level [par. 96]) (claim 10). 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 of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

10. As to claim 11, Schoen discloses a device where the 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. 30, lines 3- 7), where a visual indication is provided to the device's user to indicate the updated security mode of operation (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 device's user. 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 device's user (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 security level of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

11. As to claim 12, Schoen discloses a device where a company or government administrator uses an interface to change the configuration data stored on the centralized policy data store (par. 30, lines 3-7).

12. As to claim 13, 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 (par. 30, lines 7-10).

13. As to claim 14, 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 (par. 73, lines 16-23; Schoen; claim 9, lines 4-7).

14. As to claim 15, Schoen discloses a method for use in establishing a security-related mode of operation for computing devices, comprising: storing a security mode of operation in a policy data store (par. 69, lines 10- 15); sending the stored security mode of operation to the computing devices over a network (par. 73, lines 16-20); where the sent security mode of operation places the computing devices into one or more predetermined security-related modes of operation (par. 69, line 13-15). where at least on 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, wherein the security mode of operation forces use of one or more security algorithms. 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 security algorithms (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 of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

15. As to claim 16, Schoen discloses a method further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store (par. 60, lines 3-5).

16. As to claim 17, Schoen discloses 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 (par. 65, lines 17-21).

17. As to claim 18, Schoen discloses a method further comprising the step of receiving an indication that the devices have received and entered into the sent security mode of operation (par. 66, lines 11-13; par. 73, lines 16-23).

18. As to claim 20, Schoen discloses a digital signal containing the sent security mode of operation of claim 15 (par. 9, lines 3-6).

19. As to claim 21, 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).

20. As to claim 22, Schoen discloses 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 (Schoen: claim 4, lines 1-5; par. 32, lines 3-7); 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 (par. 9, lines 1-6). Schoen does not expressly teach the claim limitation element of a 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 security algorithms. 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 a 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 security algorithms (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 of a message disclosed above by Phillips, for which configuring devices for secure operation will be enhanced [par. 96].

21. Claims 2, 3, and 19 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).

22. As to claims 2, 3, and 19, 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 19). However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Phillips as introduced by Wencour. Wencour discloses: A system where the secure mode of operation comprises a Federal Information Processing Standard (FIPS) mode of operation (claim 2) (par. 254, lines 1-13) to provide a secure mode of operation. A system where the FIPS mode of operation includes forcing use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) (claim 3) (par. 257, lines 1-7) to provide the means to utilize encryption. 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 19) (par. 257, lines 1-7) to provide the means to utilize encryption. Therefore given the teachings of Wencour a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Phillips by employing the well known features of Federal Information Processing Standard (FIPS) and Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) disclosed above by Wencour, for which secure mode will be enhanced (par. 257, lines 1-7).

23. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Phillips, as applied to claims 1 and 5, and further in view of Lord et al. (US Patent No. 7,131,003 and Lord hereinafter).

24. As to claim 23, although the system disclose by Schoen in view of Phillips shows substantial features of the claimed invention (discussed in the paragraphs above), It fails to disclose: A system where 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 (claim 23). However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schoen and Phillips as

introduced by Lord. Lord discloses: A system where 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 (claim 23) (for purposes of policy (i.e., first security mode data structure) cryptographic operations Load provides FIPS capability [col. 5, lines 5-15] such that modification of Schoen teachings of AES and DES encryption provides enhanced security policy related operations). Therefore, given the teachings of Lord, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen and Phillips by employing the well known features of FIPS cryptographic operations disclosed above by Lord, for which security policy related operations will be enhanced [col. 5, lines 5-15]..

25. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schoen in view Phillips, as applied to claim 1, and further in view of Dutta et al. (US Patent Publication No. 20020186845 and Dutta hereinafter).

26. As to claim 24, although the system of Schoen in view of Phillips illustrates substantial features of the claim invention, the combined teaching do not disclose: 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. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schoen in view of Phillips as introduced by Dutta. Dutta 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 (to provide the capability to disable security setting through a push message (e.g., disable message) [par. 9]). Therefore, given the teachings of Dutta, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schoen in view of Phillips by employing the well known feature of using a push message to disable security features in a mobile environment disclosed above by Dutta, for which security policy related operations will be enhanced [par. 9].

Response to Amendment Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection. With regard to applicant's claim limitation element of, " ...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 security algorithms", the Examiner submits that Phillips discloses in paragraph 96, a visual indication of the security settings (i.e., mode). The security settings are visually displayed to the users.

The Examiner further submits that Phillips security setting depicts a particular security mode.

Response to Arguments

Examiner Remarks – 35 U.S.C 101

The Examiner withdraws the rejection made under 35 U.S.C. 101 in view of applicant's claim amendment.

Examiner Remarks – 35 U.S.C 103(a)

Applicant argues:

> **"these statuses are not representative of the cryptographic algorithms required by claim 1"**

The Examiner notes that paragraph 108 of the prior art discloses secure communications use cryptographic keys. Additionally the Examiner respectfully submits that the security status indicates that the communication is secure (e.g., encrypted/cryptographic algorithm).

Applicant argues:

> "**At best, Wenocur discloses as an option to use AES or 3DES to replace the SHA1 digest function. Other cryptographic functions, such as MD2, MD4, MD5, BJPE160, SHA-256, SHA- 384, SHA-512, can also be used. Thus, it never discloses the FIPS mode of operation forcing use of AES or 3DES as required by claim 3**".

The Examiner notes applicant's specification page 11 for which reads:

> **"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**".

The Examiner notes that FIPS is an abbreviation for Federal Information Processing Standards. This standard specifies the security requirement that will be satisfied by a cryptographic module utilized within a security system protecting sensitive unclassified information.

The Examiner notes that applicant's "forcing" operation is not necessary because the FIPS standard mandates specific security criteria. Therefore the Examiner contend that if FIPS practices are being adhered too, then specific cryptographic functions are required to be used in order to ensure security compliance. In this instance it is AES and 3DES. The Examiner respectfully contends that Wenocur discloses in paragraph 254 the use of FIPS compliant cryptographic functions. Furthermore, the Examiner notes that in paragraph 256, Wenocur discloses the use of both, AES and 3DES.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

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, William Korzuch can be reached on (571) 272-7589. 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

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

Index of Claims	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F 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	01/30/2008	07/18/2008	03/23/2009	11/04/2009	06/19/2010	12/04/2010			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓			
	4	✓	✓	✓	✓	✓	✓			
	5	✓	✓	✓	✓	✓	✓			
	6	✓	✓	✓	✓	✓	✓			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓			
	11	✓	✓	✓	✓	✓	✓			
	12	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓			
	14	✓	✓	✓	✓	✓	✓			
	15	✓	✓	✓	✓	✓	✓			
	16	✓	✓	✓	✓	✓	✓			
	17	✓	✓	✓	✓	✓	✓			
	18	✓	✓	✓	✓	✓	✓			
	19	✓	✓	✓	✓	✓	✓			
	20	✓	✓	✓	✓	✓	✓			
	21	✓	✓	✓	✓	✓	✓			
	22	✓	✓	✓	✓	✓	✓			
	23		✓	✓	✓	✓	✓			
	24			✓	✓	✓	✓			

FORM PTO-1449 (Modified) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	Atty Docket No.: 555255012798
	Application No.: 11/065,901
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary)	Applicant: Adams et al
	Filed: 2/25/05
(37 CFR 1.98(b))	Group: ~~2131~~ 2431 Bryan Wright

U.S. PATENT DOCUMENTS

Exam. Init.		Patent Number	Issue/Publ Date	Patentee	Class	Sub-class	Filing Date

FOREIGN PATENT OR PUBLISHED FOREIGN PATENT APPLICATION

Exam. Init.		Document Number	Publication Date of Grant	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No

OTHER DOCUMENTS (Including Author, Title, Date**, Relevant pages, Place of Publication***)

/B.W./		Supplementary European Search Report, issued 7/11/07 by European Patent Office, for European Patent App. No. 05714536
/B.W./		S. Gavrila et al, "Assigning and Enforcing Security Policies on Handheld Devices", Canadian Information Technology Security Symposium, 5/17/02, pages 0-7, XP002440113

Examiner /Bryan Wright/	Date Considered 12/04/2010

EXAMINER: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	"11067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S2	0	"11/067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S3	0	"11071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S4	2	"11/071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S5	1	"20030145214"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:39
S6	2	S4 and unique	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:40
S7	1	S5 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:46
S8	1	("7287282").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S9	1	S8 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S10	0	2005/005098	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S11	1	"2005005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S12	1	"20050005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S13	0	"11071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:01
S14	1	"11/071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S15	0	S14 and plurality	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S16	1	S14 and hardware	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S17	0	S14 and (serial same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S18	1	S14 and (image same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S19	1	S14 and (image same software same hardware)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S20	1	S12 and serial$9	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:16

S21	1	"20020010855"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:55
S22	3	"11056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:58
S23	3	"11/056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 17:00
S24	1	"20050004873"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:01
S25	4	"60,444,581"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:03
S26	0	"11067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S27	0	"11.067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S28	1	"11/067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S29	1	S28 and (print near monitor)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:47
S30	2	2003/0014368	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S31	1	S30 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S32	1	"20030014368"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S33	1	S32 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S34	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S35	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S36	1	"20030204722"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:43
S37	0	S26 and security	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:44
S38	1	S35 and (security near mode)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:00
S39	1	S36 and (securit$9)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:55
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13
S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14

S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$.DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30
S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40
S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46
S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51

S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45
S54	1	S53 and mode	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:46
S55	1	"11056219"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S56	1	"7278155"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S57	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S58	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S59	386	enable same disable same security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S60	35	S59 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S61	13	S60 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S62	105	security same mode same (deployed or deploy or deploying) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S63	97	S62 and (enabl$9 or disabl$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S64	30	S63 and security same policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S65	8628	PIM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S66	1073	S65 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S67	2	S66 and moble	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S68	724	S66 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S69	406	S68 and GSM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S70	38	S69 and security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:30

S71	144	message near server same redirected same mobile same received	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S72	130	S71 and gsm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S73	79	S72 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S74	103	pull same message same access same scheme	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S75	38	S74 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S76	10	disable same message same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:08
S77	1	11/065901	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:09
S78	68	disable same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S79	5	S78 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S80	886	disable near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13

S81	117	S80 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S82	28	S81 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S83	18	S82 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:14
S84	4	("6219694").pn. or ("7065347").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:23
S85	402	redirection near server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S86	146	S85 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S87	27	S86 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S88	15	S87 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S89	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:51
S90	40	(disable near (message or signal or notification) same disabling same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:58

S91	2	S90 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 11:01
S92	15723	(disable near (message or signal or notification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S93	511	S92 and GSM	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S94	8	S93 and security near4 setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S95	57	S93 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:35
S96	1308	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 13:08
S97	1112	configuration near3 message same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:12
S98	0	S97 and visual near3 indication same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S99	39	visual near3 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S100	10	S99 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13

S101	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
S102	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
S103	39	visual near5 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S104	10	S103 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S105	603	visual near5 indication and security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S106	237	S105 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S107	128	S106 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S108	4	S106 and push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S109	3	"20050020244"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S110	1565	configuration near message and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21

S111	3	S110 and visual same setting same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
S112	2	S110 and security same setting same displayed same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
S113	1739	push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S114	0	S113 and visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S115	237	visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S116	54	S115 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:24
S117	375	visual same security same (setting or mode) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S118	111	S117 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S119	111	S118	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S120	31	S118 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25

S121	25809	security same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S122	8744981	S121 an(d visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S123	1195	S121 and (visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S124	369	S123 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S125	157	S124 and (security same (mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S126	87	S125 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:28
S127	225	S124 and (security same (mode or setting or level))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S128	135	S127 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S129	8064	visual same indication same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S130	1602	S129 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32

S131	390	S130 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S132	200	S131 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S133	132	S131 and (security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S134	20	S131 and (security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S135	2059	(security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S136	301	(security same (level or mode or setting)) same visual same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S137	238	S136 and config$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S138	128	S136 and (config$9 same (message or instruct$9 or setting)) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:35
S139	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S140	1082101	S139 and display$9 or visual$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41

S141	2	S139 and (display$9 or visual$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S142	551	(visual$9 same (indicate or indication or indicator) same security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:43
S143	389	S142 and configur$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S144	97	S143 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S145	17	S144 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:46
S146	8093	device same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S147	2647	S146 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S148	167	S147 and (visual$5 near (indicator or indication or indicate))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S149	1054	(security near3 (indicator or indication or indicate) near4 (mode or level or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S150	48	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53

S151	124	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display $9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S152	34	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display $9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S153	192	icon same encrypted same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S154	119	icon same encrypted same message same user	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S155	52	S154 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S156	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 10:20
S157	2	"20030204722"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/30 14:29
S158	1	"10592339"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/31 16:48
S159	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:27
S160	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:27

S161	13	(mobile same device same security near mode same (display or visual))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:28
S162	800	(security same (mode or setting)) and FIPS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S163	135	(security same (mode or setting)) same FIPS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S164	38	(security same (mode or setting)) same FIPS same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S165	7	S164 and (visual or display) same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S166	524	fips and (visual or display) same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:36
S167	524	(fips and (visual or display) same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:36
S168	60	S167 and deployed same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:36
S169	393	(configur$9 same device same (security)) and FIPS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:40
S170	0	S159 and ((diplay or visual) same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:40

S171	0	S159 and ((display or visual) same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:40
S172	422	((display or visual) same indicating same security same (setting or mode))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:41
S173	0	S172 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:41
S174	176	((display or visual) same indicating same security same (setting or mode) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:41
S175	99	S174 and ((mobile or wireless) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:43
S176	729744	((mobile or wireless) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:46
S177	1368	S176 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:46
S178	4	S177 and (security same (mode or setting)) same icon	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:47
S179	5	fips and (security same (mode or setting)) same icon	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:49
S180	7	fips and (security same (visual or mode or setting)) same icon	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:49

S181	42	fips and (security same (visual or mode or setting)) same displayed	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:49
S182	19	disabl$5 near security and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:52
S183	0	(security near icon same indicating same (security near (mode or settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:56
S184	2	(security same icon same indicating same (security near (mode or settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:57
S185	13	(security same icon same indicating same (security near (mode or settings or status)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:57
S186	12	(security same visual same indicating same (security near (mode or settings or status)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:58
S187	39	(security same visual same (indicating or indication) same (security near (mode or settings or status)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:59
S188	22	S187 and ((wireless or mobile) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 17:00
S189	1899	(726/1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 08:53
S190	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 08:56

S191	1	"11/065901"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO; DERWENT;
			IBM_TDB
				OR	ON	2010/06/19
						08:56

12/4/2010 11:37:44 PM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

Search Notes	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F WRIGHT	**Art Unit** 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright
726	1	3/23/2009	Bryan Wright
726	1	6/19/2010	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203	1/29/2008	Bryan Wright
Additional search class/subclass 713/168	7/18/2008	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	3/23/2009	Bryan Wright
Additional search class/subclass 380/247	3/23/2009	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	6/19/2010	Bryan Wright
Additional search class/subclass 380/247, 726/11	6/19/2010	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	2431
Examiner	:	Bryan F. Wright

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSIVE AMENDMENT

Dear Sir:

This responsive amendment is filed in response to the final Office action dated January 24, 2011. Please amend the above-identified application as follows and consider the remarks contained herein. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

IN THE CLAIMS

1. (Currently Amended) 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. (Previously Presented) 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. (Currently Amended) The system of claim 1, further comprising an administrator interface for updating the configuration data related to a plurality of computing devices that is stored in the policy data store and for communicating security modes of operation to the plurality of computing devices;

wherein 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;

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.

7. (Original) The system of claim 6, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Previously Presented) 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.

9. (Original) The device of claim 8, 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.

10. (Previously Presented) The device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. (Original) The device of claim 10, 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.

12. (Previously Presented) The device of claim 11, further comprising an administrator interface for changing the configuration data stored on the centralized policy data store.

13. (Original) The device of claim 8, 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.

14. (Original) The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Previously Presented) 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.

16. (Original) The method of claim 15, further comprising the step of enabling an administrator to configure the security mode of operation stored in the policy data store.

17. (Previously Presented) The method of claim 15, 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.

18. (Previously Presented) The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. (Original) The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20. (Original) A digital signal containing the sent security mode of operation of claim 15.

21. (Previously Presented) 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 15.

22. (Previously Presented) 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.

23. (Previously Presented) 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.

24. (Previously Presented) 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.

REMARKS

Claims 1-24 are pending in the instant application and stand rejected. Claims 1 and 6 are amended to make the claim language consistent. Reconsideration is respectfully requested in light of the following remarks.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 4-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2003/0204722, application of Schoen, et al. (Schoen), in view of U.S. Publication No. 2005/0183138, application of Philips et al. (Philips). Claims 2-3 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen in view of Philips in further view of U.S. Publication No. 2002/0165912, application of Wenocur, et al. (Wenocur). Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Philips in further view of U.S. Patent No. 7,131,003 (Lord). Claim 24 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schoen view of Philips in further view of U.S. Patent Publication No. 2002/0186845 (Dutta). Assignee respectfully disagrees with the rejections.

Claim 1 is directed to a system for establishing a security-related mode of operation for computing devices. Claim 1 requires that the computing devices comprise user interface instructions configured to send an output to a display associated with the computing device, where the output is configured to comprise a visual indication of the security mode of operation of the user device to the user of the device, and the security mode of operation forces use of one or more cryptographic algorithms. The Office cites to paragraph [0096] of Philips as disclosing such a feature. The cited paragraph 0096 of Philips states:

> [0096] Status indicators 910-916 are included to provide a visual indication of the network security module's current status. Status indicators, as previously discusses, are for informational purposes only. They provide optional visual clues to the computer user as to the

> protective security measures implemented by the network security module 304. Each indicator corresponds to a particular security status. For example, status indicator 910 may correspond to a security level of red, meaning a total lock-down of network activities, and is illuminated in red when the network security module 304 is implementing a total lock-down. Status indicator 912 may correspond to a security level of yellow, i.e., a partial lock-down of network activities, and be illuminated in yellow when the network security module 304 is implementing the partial lock-down. Similarly, status indicator 914 may correspond to the security level green, i.e., free network access, and is illuminated in green when the network security module 304 is permitting unrestricted network access. Status indicator 916 may correspond to the enabled/disabled status of the network security module 304, such that the status indicator is illuminated, perhaps as with a flashing red light, when the network security module is disabled.

The cited portion of Philips merely discloses a group of status indicators that identify the statuses of the network, such as a total lock-down of network activities, a partial lock-down of network activities, and unrestricted network access. These network statuses indicators, at best, show whether communications between a device and other entities in the network are blocked or permitted. The operation mode of a particular device itself is not affected by network statuses. See paragraphs 0049, 0050, and 0069 of Philips. Thus, the network status indicators do not indicate a security mode of operation of a particular device as required by claim 1.

Further, claim 1 requires a security mode of operation forces use of one or more cryptographic algorithms. The above-discussed portion of Philips never discloses that a mode of operation of a particular device forces use of specific cryptographic algorithms. In the Response to Arguments of the final Office Action, the Office cites to paragraph 108 of Philips as teaching "secure communications use cryptographic keys." The cited paragraph 108 of Philips states:

> [0108] As an example of how computer exploits may be delivered to a computing device using secured communications, and with reference to FIG. 11, a malicious party on computer 102 has an exploit 112. In order to infect another computer, such as computer 1104, the malicious party may offer the exploit 112 as a legitimate resource/content to others, but offers to deliver it via secured communications. As is known to those skilled in

> the art, secured communications are encrypted, typically with public and private cryptographic keys, such that only the possessor of a decryption key (the private key) is able to decrypt and view the content of the secured communications. Examples of secured communication protocols include Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols.

It is true that the cited paragraph 108 of Philips is related to secure communications using cryptographic keys. However, this paragraph merely discusses how computer exploits attempt to infect a computer by requesting delivery via secured communications, and does not disclose that a security mode of operation of a particular device forces use of one or more cryptographic algorithms as required by claim 1. Because the cited references, singly or in combination, fail to disclose the above-noted feature of claim 1, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

Independent claims 8, 15, 22 recite similar features as claim 1. These claims are allowable for at least the same reasons as offered for claim 1.

Moreover, the Office fails to make a prima facie unpatentability case against certain dependent claims. For example, claim 4 recites that 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, and the second security mode data structure includes a second security mode being associated with a second plurality of computing devices. In rejecting claim 4, the Office cites to lines 16-23 in paragraph 0073 of Schoen. The cited portion of Schoen discloses that administrators create instant messaging policy certificates, and then publish the certificates or broadcast the certificates to the instant messaging devices. However, the cited portion of Schoen does not disclose providing different certificates for different instant messaging devices.

Moreover, though the certificates may result in changes to the configuration data of the instant messaging devices, such as whether access of some subscribers is permitted, see Figure 11 and paragraphs 0074-0076, the security modes of operation of the devices are not affected by the certificates. Thus, Schoen does not disclose the features of claim 4. The other cited references do not make up for Schoen's deficiency. Because the cited references do not disclose the features of claim 4, it is respectfully requested that the § 103 rejection of claim 4 be withdrawn.

It should be noted that assignee has not presented arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to assignee's right to present arguments to all of the dependent claims at any point in the future. In addition, because each of the dependent claims depends from a base claim that is itself allowable, the dependent claims are allowable for at least these reasons and should proceed to issuance.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Date: March 24, 2011

Respectfully submitted,

John V. Biernacki (Reg. No. 40,511)
Jones Day
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939

Electronic Acknowledgement Receipt

EFS ID:	9734432
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
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/John V. Biernacki
Filer Authorized By:	Stephen D. Scanlon
Attorney Docket Number:	555255012798
Receipt Date:	24-MAR-2011
Filing Date:	25-FEB-2005
Time Stamp:	16:58:55
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	Amendment After Final	012798.pdf	433673 4aa12c37e311bb4fae53e413987a9bb5cda43592	no	13

Warnings:

Information:

Total Files Size (in bytes):	433673

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.

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 11/065,901	Filing Date 02/25/2005	□ 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	**03/24/2011**	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	** 25	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	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:
/DONNA D. SMALLS LOGAN/

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.

Attorney Docket No. 555255-012798

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Neil P. Adams
Serial No.	:	11/065,901
Filing Date	:	February 25, 2005
For	:	System and Method for Configuring Devices for Secure Operations
Art Unit	:	2431
Examiner	:	Bryan F. Wright

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSIVE AMENDMENT

Dear Sir:

This responsive amendment is filed in response to the final Office action dated January 24, 2011. Please amend the above-identified application as follows and consider the remarks contained herein. Any fees due should be charged to Jones Day Deposit Account No. 501432, ref: 555255-012798.

OK TO ENTER: /B.W./

04/05/2011

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	56662	726/1 726/3 726/4 726/2 713/189 713/165 713/168 455/410 455/411 726/11 707/100 380/277 713/188 713/167 713/193 726/27 726/28 726/22	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:02
L5	9	l4 and ((device or apparatus) same (secure or security) near3 mode same policy same (indication or indicator or indicating or display$8 or visual))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/05 11:04
S1	0	"11067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S2	0	"11/067583"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 13:29
S3	0	"11071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S4	2	"11/071252"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:38
S5	1	"20030145214"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:39
S6	2	S4 and unique	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:40
S7	1	S5 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:46
S8	1	("7287282").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S9	1	S8 and id	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 14:48
S10	0	2005/005098	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S11	1	"2005005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S12	1	"20050005098"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 15:34
S13	0	"11071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:01

S14	1	"11/071079"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S15	0	S14 and plurality	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S16	1	S14 and hardware	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:02
S17	0	S14 and (serial same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S18	1	S14 and (image same software)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S19	1	S14 and (image same software same hardware)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:06
S20	1	S12 and serial$9	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:16
S21	1	"20020010855"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:55
S22	3	"11056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 16:58
S23	3	"11/056928"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/10 17:00
S24	1	"20050004873"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:01
S25	4	"60,444,581"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/11 13:03
S26	0	"11067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S27	0	"11.067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S28	1	"11/067081"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:46
S29	1	S28 and (print near monitor)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:47
S30	2	2003/0014368	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S31	1	S30 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 12:58
S32	1	"20030014368"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S33	1	S32 and post	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:00
S34	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S35	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:42
S36	1	"20030204722"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:43

S37	0	S26 and security	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 13:44
S38	1	S35 and (security near mode)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:00
S39	1	S36 and (securit$9)	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 14:55
S40	409	(FIPS near "140")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:13
S41	215	S40 and (policy or policies or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S42	45	S41 and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:14
S43	2	US-6202157-$.DID. OR US-6732168-$.DID. OR WO-0069120-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2008/07/12 16:20
S44	21121	(FIPS)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:30
S45	15423	S44 and (AES or DES)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:31
S46	5	"0069120"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:40
S47	0	S46 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41
S48	0	S47 and aes	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:41

S49	21121	fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:46
S50	514	FIPS and security and AES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:48
S51	134	S50 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:49
S52	57	S51 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/07/12 16:51
S53	1	("7131003").pn.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:45
S54	1	S53 and mode	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 17:46
S55	1	"11056219"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S56	1	"7278155"	US-PGPUB; USPAT; EPO	OR	ON	2008/07/12 18:17
S57	0	"11065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S58	1	"11/065901"	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:15
S59	386	enable same disable same security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S60	35	S59 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S61	13	S60 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:19
S62	105	security same mode same (deployed or deploy or deploying) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S63	97	S62 and (enabl$9 or disabl$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25

S64	30	S63 and security same policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:25
S65	8628	PIM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S66	1073	S65 and policy	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S67	2	S66 and moble	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S68	724	S66 and mobile	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S69	406	S68 and GSM	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:29
S70	38	S69 and security same mode	US-PGPUB; USPAT; EPO	OR	ON	2009/03/22 21:30
S71	144	message near server same redirected same mobile same received	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S72	130	S71 and gsm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S73	79	S72 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:35
S74	103	pull same message same access same scheme	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S75	38	S74 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/22 21:41
S76	10	disable same message same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:08

S77	1	11/065901	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:09
S78	68	disable same disabling same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S79	5	S78 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:12
S80	886	disable near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S81	117	S80 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S82	28	S81 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:13
S83	18	S82 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:14
S84	4	("6219694").pn. or ("7065347").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:23
S85	402	redirection near server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44
S86	146	S85 and e$mail	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:44

S87	27	S86 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S88	15	S87 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:45
S89	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:51
S90	40	(disable near (message or signal or notification) same disabling same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 10:58
S91	2	S90 and email	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 11:01
S92	15723	(disable near (message or signal or notification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S93	511	S92 and GSM	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S94	8	S93 and security near4 setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:33
S95	57	S93 and policy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 12:35
S96	1308	(726/1).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/23 13:08

S97	1112	configuration near3 message same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:12
S98	0	S97 and visual near3 indication same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S99	39	visual near3 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S100	10	S99 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:13
S101	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
S102	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:15
S103	39	visual near5 indication same security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S104	10	S103 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:17
S105	603	visual near5 indication and security same setting	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S106	237	S105 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18

S107	128	S106 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S108	4	S106 and push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:18
S109	3	"20050020244"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S110	1565	configuration near message and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:21
S111	3	S110 and visual same setting same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
S112	2	S110 and security same setting same displayed same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:22
S113	1739	push near message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S114	0	S113 and visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S115	237	visual same security same mode same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:23
S116	54	S115 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:24

S117	375	visual same security same (setting or mode) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S118	111	S117 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S119	111	S118	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S120	31	S118 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:25
S121	25809	security same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S122	8744981	S121 an(d visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S123	1195	S121 and (visual near (display or indictor or indication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:26
S124	369	S123 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S125	157	S124 and (security same (mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:27
S126	87	S125 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:28

S127	225	S124 and (security same (mode or setting or level))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S128	135	S127 and config$9 same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:29
S129	8064	visual same indication same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S130	1602	S129 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S131	390	S130 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S132	200	S131 and security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:32
S133	132	S131 and (security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S134	20	S131 and (security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S135	2059	(security same (level or mode or setting)) same visual	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:33
S136	301	(security same (level or mode or setting)) same visual same display$9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34

S137	238	S136 and config$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:34
S138	128	S136 and (config$9 same (message or instruct$9 or setting)) same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:35
S139	3	"20050190764"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S140	1082101	S139 and display$9 or visual$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S141	2	S139 and (display$9 or visual$9)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:41
S142	551	(visual$9 same (indicate or indication or indicator) same security same (level or mode or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:43
S143	389	S142 and configur$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S144	97	S143 and push	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:44
S145	17	S144 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:46
S146	8093	device same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48

S147	2647	S146 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S148	167	S147 and (visual$5 near (indicator or indication or indicate))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:48
S149	1054	(security near3 (indicator or indication or indicate) near4 (mode or level or setting))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S150	48	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:53
S151	124	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display $9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S152	34	(security near3 (indicator or indication or indicate) near4 (mode or level or setting)) same display $9 same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 10:54
S153	192	icon same encrypted same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S154	119	icon same encrypted same message same user	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S155	52	S154 and mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/25 11:04
S156	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 10:20

S157	2	"20030204722"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/30 14:29
S158	1	"10592339"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/31 16:48
S159	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:27
S160	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:27
S161	13	(mobile same device same security near mode same (display or visual))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:28
S162	800	(security same (mode or setting)) and FIPS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S163	135	(security same (mode or setting)) same FIPS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S164	38	(security same (mode or setting)) same FIPS same device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S165	7	S164 and (visual or display) same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:34
S166	524	fips and (visual or display) same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:36

S167	524	(fips and (visual or display) same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:36
S168	60	S167 and deployed same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:36
S169	393	(configur$9 same device same (security)) and FIPS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:40
S170	0	S159 and ((diplay or visual) same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:40
S171	0	S159 and ((display or visual) same security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:40
S172	422	((display or visual) same indicating same security same (setting or mode))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:41
S173	0	S172 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:41
S174	176	((display or visual) same indicating same security same (setting or mode) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:41
S175	99	S174 and ((mobile or wireless) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:43
S176	729744	((mobile or wireless) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:46

S177	1368	S176 and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:46
S178	4	S177 and (security same (mode or setting)) same icon	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:47
S179	5	fips and (security same (mode or setting)) same icon	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:49
S180	7	fips and (security same (visual or mode or setting)) same icon	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:49
S181	42	fips and (security same (visual or mode or setting)) same displayed	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:49
S182	19	disabl$5 near security and fips	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:52
S183	0	(security near icon same indicating same (security near (mode or settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:56
S184	2	(security same icon same indicating same (security near (mode or settings)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:57
S185	13	(security same icon same indicating same (security near (mode or settings or status)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:57
S186	12	(security same visual same indicating same (security near (mode or settings or status)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:58

S187	39	(security same visual same (indicating or indication) same (security near (mode or settings or status)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 16:59
S188	22	S187 and ((wireless or mobile) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 17:00
S189	1899	(726/1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 08:53
S190	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 08:56
S191	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 08:56
S192	2	"20030204722"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/12/17 22:31
S193	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/12/17 22:31
S194	37	"20020165912"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/12/17 22:53
S195	2	"11065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:50
S196	1	"11/065901"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:50

S197	56381	adams.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:50
S198	10665	S197 and forces	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:51
S199	58	S198 and cryptographic $9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:51
S200	30	S199 and admin$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:51
S201	8	S200 and indication same admin$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:51
S202	4141	(enable or enabling) same security same mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:53
S203	299	(enable or enabling) near5 security near4 mode	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:54
S204	177	S203 and display	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:54
S205	97	S203 and display$9 same security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:54
S206	29	S203 and display$9 near4 security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:54

S207	18	S206 and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:54
S208	453	configur$9 near4 secure near5 operation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:57
S209	177	S208 and disabl$9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 14:57
S210	3	"20050015604"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:23
S211	2	("6718024").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:23
S212	24	activate near4 secure near5 mode same device and wireless	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:23
S213	107	((enbable or enabling or enabled or activat$9 or configur$9) near4 secure near5 mode same device and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:28
S214	20619	726/1 726/4 726/2 713/189 713/165 455/410 455/411	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:35
S215	899	S214 and secure near4 operation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:36
S216	30	S215 and ((enbable or enabling or enabled or activat$9 or configur $9) near4 secure near5 mode and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:37

S217	22142	726/1 726/3 726/4 726/2 713/189 713/165 455/410 455/411	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:37
S218	30	S216 and ((enbable or enabling or enabled or activat$9 or configur$9) near4 secure near5 mode and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:38
S219	776	((enbable or enabling or enabled or activat$9 or configur$9) near4 (secure or security) near5 mode and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:38
S220	853	((enable or enabling or enabled or activat$9 or configur$9) near4 (secure or security) near5 mode and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:38
S221	679085	((enable or enabling or enabled or activat$9 or configur$9) near4 (secure or security) near5 mode samd device and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:39
S222	395	((enable or enabling or enabled or activat$9 or configur$9) near4 (secure or security) near5 mode same device and wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:39
S223	302	S222 and ((indicate or indication or visual or display$9) same mode)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:40
S224	41	S223 and cryptographic $9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:40
S225	26932	726/1 726/3 726/4 726/2 713/189 713/165 713/168 455/410 455/411	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/04 15:43

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	27327	726/1 726/3 726/4 726/2 713/189 713/165 713/168 455/410 455/411	US-PGPUB; USPAT; UPAD	OR	ON	2011/04/05 10:42
L2	1	l1 and ((device or apparatus) same (secure or security) near3 mode same policy same (indicat $8 or visual) same admin$9)	US-PGPUB; USPAT; UPAD	OR	ON	2011/04/05 10:46
L3	5	l1 and ((device or apparatus) same (secure or security) near3 mode same policy same (indicat $8 or visual))	US-PGPUB; USPAT; UPAD	OR	ON	2011/04/05 10:47
L6	0	"l4" and ((device or apparatus) same (secure or security) near3 mode same policy same (indication or indicator or indicating or display$8 or visual))	US-PGPUB; USPAT; UPAD	OR	ON	2011/04/05 11:05
L7	19	((device or apparatus) same (secure or security) near3 mode same policy same (indication or indicator or indicating or display$8 or visual))	US-PGPUB; USPAT; UPAD	OR	ON	2011/04/05 11:05

4/5/2011 11:30:40 AM
C:\ Documents and Settings\ bwright\ My Documents\ EAST\ Workspaces\ 11065901.wsp

Search Notes	Application/Control No. 11065901	Applicant(s)/Patent Under Reexamination ADAMS ET AL.
	Examiner BRYAN F WRIGHT	Art Unit 2431

SEARCHED

Class	Subclass	Date	Examiner
726	1	1/30/2008	Bryan Wright
726	1	3/23/2009	Bryan Wright
726	1	6/19/2010	Bryan Wright
726	1	4/5/2011 (updated search)	Bryan Wright

SEARCH NOTES

Search Notes	Date	Examiner
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	1/29/2008	Bryan Wright
Additional class/subclass search: 726/4, 713/201, 713/156, 709/203	1/29/2008	Bryan Wright
Additional search class/subclass 713/168	7/18/2008	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	3/23/2009	Bryan Wright
Additional search class/subclass 380/247	3/23/2009	Bryan Wright
automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	6/19/2010	Bryan Wright
Additional search class/subclass 380/247, 726/11	6/19/2010	Bryan Wright
Text search using automated search tools USPTO, USPG, EPO, JPO, Derwent, IBM Technical, Non-patent literature	4/5/2011	Bryan Wright
Limited text search class/subclass 726/1 726/3 726/4 726/2 713/189 713/165 713/168 455/410 455/411 726/11 707/100 380/277 713/188 713/167 713/193 726/27 726/28 726/22	4/5/2011	Bryan Wright

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	1-4, 11, 22, 27, 28	4/5/2011	Bryan Wright
713	165, 167, 188, 193	4/5/2011	Bryan Wright
707	100	4/5/2011	Bryan Wright
380	277	4/5/2011	Bryan Wright
455	410, 411	4/5/2011	Bryan Wright

Interference search noted /B. W./ Examiner.Art Unit 2431	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11065901	ADAMS ET AL.
	Examiner	**Art Unit**
	BRYAN WRIGHT	2431

ORIGINAL

CLASS	SUBCLASS
726	1

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	2	3	4	11	22
726	27	28			
713	165	167	188	189	193
380	277				
455	410	411			

INTERNATIONAL CLASSIFICATION

CLAIMED					NON-CLAIMED				
G	0	6	F	17 / 00 (2006.01.01)	G	0	6	F	17 / 00 (2006.01.01)
H	0	4	L	29 / 06 (2006.01.01)	H	0	4	L	29 / 06 (2006.01.01)

□ **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	24												
2	2	18	25												
3	3														
4	4														
5	5														
6	7														
7	8														
8	10														
9	11														
10	13														
11	14														
12	15														
13	18														
14	19														
15	22														
16	23														

/BRYAN WRIGHT/ Examiner.Art Unit 2431 (Assistant Examiner)	4/5/2011 (Date)	**Total Claims Allowed:** 18	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2468 (Primary Examiner)	04/11/2011 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office

Part of Paper No. 20110404

Index of Claims	**Application/Control No.** 11065901	**Applicant(s)/Patent Under Reexamination** ADAMS ET AL.
	Examiner BRYAN F 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	01/30/2008	07/18/2008	03/23/2009	11/04/2009	06/19/2010	12/04/2010	04/05/2011		
1	1	✓	✓	✓	✓	✓	✓	=		
2	2	✓	✓	✓	✓	✓	✓	=		
3	3	✓	✓	✓	✓	✓	✓	=		
4	4	✓	✓	✓	✓	✓	✓	=		
5	5	✓	✓	✓	✓	✓	✓	=		
	6	✓	✓	✓	✓	✓	✓	-		
6	7	✓	✓	✓	✓	✓	✓	=		
7	8	✓	✓	✓	✓	✓	✓	=		
	9	✓	✓	✓	✓	✓	✓	-		
8	10	✓	✓	✓	✓	✓	✓	=		
9	11	✓	✓	✓	✓	✓	✓	=		
	12	✓	✓	✓	✓	✓	✓	-		
10	13	✓	✓	✓	✓	✓	✓	=		
11	14	✓	✓	✓	✓	✓	✓	=		
12	15	✓	✓	✓	✓	✓	✓	=		
	16	✓	✓	✓	✓	✓	✓	-		
	17	✓	✓	✓	✓	✓	✓	-		
13	18	✓	✓	✓	✓	✓	✓	=		
14	19	✓	✓	✓	✓	✓	✓	=		
	20	✓	✓	✓	✓	✓	✓	-		
	21	✓	✓	✓	✓	✓	✓	-		
15	22	✓	✓	✓	✓	✓	✓	=		
16	23		✓	✓	✓	✓	✓	=		
17	24			✓	✓	✓	✓	=		
18	25							=		

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 04/18/2011

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

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	**PAPER NUMBER**
2431	

DATE MAILED: 04/18/2011

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

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	$1510	$300	$0	$1810	07/18/2011

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 04/18/2011

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

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	$1510	$300	$0	$1810	07/18/2011

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 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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

89441 7590 04/18/2011

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

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 04/18/2011

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 556 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 556 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.** 11/065,901	**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 *3/24/2011*.

2. ☒ The allowed claim(s) is/are *1-5,7,8,10,11,13-15,18,19 and 22-25*.

3. □ 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.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ 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. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *March 31, 2011* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

/BRYAN WRIGHT/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2468

Examiner-Initiated Interview Summary	**Application No.** 11/065,901	**Applicant(s)** ADAMS ET AL.	
	Examiner BRYAN WRIGHT	**Art Unit** 2431	

All Participants:

(1) BRYAN WRIGHT.

(2) _____.

Status of Application: Flnal

(3) Mathhew Johnson Reg. No. 59,108.

(4) _____.

Date of Interview: 21 March 2011

Time: noon

Type of Interview:
☒ Telephonic
☐ Video Conference
☐ Personal (Copy given to: ☐ Applicant ☒ Applicant's representative)

Exhibit Shown or Demonstrated: ☐ Yes ☒ No
If Yes, provide a brief description: .

Part I.

Rejection(s) discussed:
35 U.S.C. 103(a)

Claims discussed:
1, 6, 8, 15, 22

Prior art documents discussed:
Schoen et al. (US Patent Publication No. 2003/0204722) and Phillips et al. (US Patent Publication No. 2005/0183138).

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
Proposed amendment to place the application in condition for allowance.

Part III.

☒ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.

☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

(Applicant/Applicant's Representative Signature – if appropriate)

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mathew Johnson on reg. no. 59,108 on March 31, 2011.

1. The following claims listed below supersedes all previous claim version

1. A system for 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 for at least one of the plurality of computing device;

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;

wherein an administrator interface is configured to update the configuration data stored in the policy data store and for communicating security modes of operation to the plurality of computing devices, wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data.

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. (Cancelled).

7. The system of claim 1, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. 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;

wherein an administrator interface is configured to update the configuration data stored in the policy data store and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated configuration data.

9. (Cancelled)

10. The device of claim 9, wherein the visual indication of the security mode is provided by a security options screen.

11. The device of claim 10, 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.

12. (Cancelled).

13. The device of claim 8, 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.

14. The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. A method for 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;

wherein an administrator interface is configured to update the security mode stored in the policy data store and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated security mode.

16-17. (Cancelled).

18. The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20-21. (Cancelled)

22. 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;

wherein an administrator interface is configured to update the security mode and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated security mode.

23. 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.

24. 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.

25. A non-transitory computer-readable media programmed with instructions for commanding one or more data processors to execute a method for establishing a security-related mode of operation for computing devices, 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;

wherein an administrator interface is configured to update the security mode stored in the policy data store and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated security mode.

REASONS FOR ALLOWANCE

2. The Examiner finds applicant's amendment to independent claim 1 to be sufficient to overcome the cited prior art of Schoen et al. (US Patent Publication No. 2003/0204722) and Phillips et al. (US Patent Publication No. 2005/0183138). The Examiner notes that the teachings of Schoen and Phillips do not teach nor make obvious applicant's claim limitation elements of: "wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data". Additionally the Examiner notes that neither reference discloses applicant's claim limitation elements of: "wherein the security mode of operation places the plurality of computing devices in a predetermined security mode of operation" and "wherein the security mode of operation forces use of one or more cryptographic algorithms". The Examiner notes that applicant's rep. added independent claim 25 as part of the claim amendment dated March 31, 2011. Independent claim 25 includes the claim limitation elements of: "wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data" and " wherein the security mode of operation forces use of one or more cryptographic algorithms". The Examiner notes that the above claim limitations contained within independent claim 25 are not taught by the cited prior art of Schoen and Phillips.

3. The Examiner finds applicant's amendment to independent claims 8 and 15 to be sufficient to overcome the cited prior art of Schoen et al. (US Patent Publication No.

2003/0204722) and Phillips et al. (US Patent Publication No. 2005/0183138). The Examiner notes that the teachings of Schoen and Phillips do not teach nor make obvious applicant's claim limitation elements of: "wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data". Additionally the Examiner notes that neither reference discloses applicant's claim limitation element of: "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".

3. The Examiner finds applicant's amendment to independent claim 22 to be sufficient to overcome the cited prior art of Schoen et al. (US Patent Publication No. 2003/0204722) and Phillips et al. (US Patent Publication No. 2005/0183138). The Examiner notes that the teachings of Schoen and Phillips do not teach nor make obvious applicant's claim limitation elements of: "wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data". Additionally the Examiner notes that neither reference discloses applicant's claim limitation element of: "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".

3. The Examiner notes the prior reference of Dahan et al (US Patent Publication No. 2004/0123118). This reference was obtained from an updated prior art search. Dahan discloses a secure mode indicator on a wireless device, however Dahan teachings do not disclose applicant's claim limitation elements of: “wherein the security mode of operation forces use of one or more cryptographic algorithms” and “wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data”. The Examiner additionally notes prior art reference Shelest et al. (US Patent No. 7,591,002). Shelest was obtained from an interference search. The Examiner notes Shelest discloses sending security policy related data to a computing system, however Shelest teachings do not disclose applicant’s claim limitation elements of: “wherein the security mode of operation forces use of one or more cryptographic algorithms”, “displaying the security mode of operation to a user of the computing device through a display associated with the computing device” and “wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data”.

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 1-5, 7, 8, 10, 11, 13-15, 18, 19 and 22-25 are allowed.

Interview Summary

The Examiner contacted applicant's rep. on March 30, 2011 concerning a proposed claim amendment to overcome the prior art. The Examiner proposed adding the subject matter contained in dependent claim 6 to each independent claim. Applicant's rep. agreed to the proposed amendment after consultation with their clients. The amendment is captured above in an Examiner 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, Nathan Flynn 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

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2468

Notice of References Cited	Application/Control No. 11/065,901	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-2004/0123118	06-2004	Dahan et al.	713/189
*	B	US-7,591,002	09-2009	Shelest et al.	726/1
	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.

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. 4175

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/065,901	02/25/2005 **RULE**	726	2431	555255012798

APPLICANTS

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

** **CONTINUING DATA** *************************

This appln claims benefit of 60/567,137 04/30/2004

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** **

06/01/2005

Foreign Priority claimed □ Yes ☑ No 35 USC 119(a-d) conditions met □ Yes ☑ No Verified and Acknowledged /BRYAN F WRIGHT/ Examiner's Signature	□ Met after Allowance Initials	**STATE OR COUNTRY** CANADA	**SHEETS DRAWINGS** 10	**TOTAL CLAIMS** 22	**INDEPENDENT CLAIMS** 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 1584	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

BIB (Rev. 05/07).

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination	
11065901	ADAMS ET AL.	
Examiner	Art Unit	
BRYAN WRIGHT	2431	

ORIGINAL	
CLASS	SUBCLASS
726	1

INTERNATIONAL CLASSIFICATION									
CLAIMED					NON-CLAIMED				
G	0	6	F	17 / 00	G	0	6	F	17 / 00
H	0	4	L	29 / 06	H	0	4	L	29 / 06

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	2	3	4	11	22
726	27	28			
713	165	167	188	189	193
380	277				
455	410	411			

□ 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	24												
2	2	18	25												
3	3														
4	4														
5	5														
6	7														
7	8														
8	10														
9	11														
10	13														
11	14														
12	15														
13	18														
14	19														
15	22														
16	23														

/BRYAN WRIGHT/ Examiner.Art Unit 2431 (Assistant Examiner)	4/5/2011 (Date)	Total Claims Allowed: 18	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2468 (Primary Examiner)	04/11/2011 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

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 04/18/2011

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

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	$1510	$300	$0	$1810	07/18/2011

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 Krishna K. Pathiyal
3 Robert C. Liang

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 Matthew W. Johnson Date July 14, 2011

Typed or printed name Matthew W. Johnson Registration No. 59,108

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:	11065901
Filing Date:	25-Feb-2005
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:	555255012798

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	1510	1510
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1810**

Electronic Acknowledgement Receipt

EFS ID:	10521352
Application Number:	11065901
International Application Number:	
Confirmation Number:	4175
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:	555255012798
Receipt Date:	14-JUL-2011
Filing Date:	25-FEB-2005
Time Stamp:	15:36:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1810
RAM confirmation Number	2059
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 1.19 (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)	012798_fee.pdf	169786 15904277a94f8bc627b7e8dcbc376672c0bd90c0	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32321 d0d9fa4ee7e12f1d7580d31c4989ef97208a7ec7	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	202107	

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.

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.
11/065,901	02/25/2005	Neil P. Adams	555255012798	4175

89441 7590 07/27/2011

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
07/27/2011	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

Supplemental Notice of Allowability	**Application No.** 11/065,901	**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 _____.

2. ☒ The allowed claim(s) is/are *1-5,7,8,10,11,13-15,18,19 and 22-25*.

3. □ 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.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ 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. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. □ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

SUPPLEMENTAL EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The following claims listed below supersedes all previous claim version and is submitted to correct the dependency of claim 10.

1. (Currently Amended) A system for 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 for at least one of the plurality of computing device;

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;

wherein an administrator interface is configured to update the configuration data stored in the policy data store and for communicating security modes of operation to the plurality of computing devices, wherein the administrator interface provides an indication that the plurality of computing devices have entered into a security mode that is compliant with the updated configuration data.

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. (Cancelled).

7. The system of claim 1, wherein the plurality of computing devices are devices from a group that includes mobile devices, desktop devices, and combinations thereof.

8. (Currently Amended) 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;

wherein an administrator interface is configured to update the configuration data stored in the policy data store and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated configuration data.

9. (Cancelled)

10. (Currently Amended) The device of claim **[9]** **8**, wherein the visual indication of the security mode is provided by a security options screen.

11. The device of claim 10, 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.

12. (Cancelled).

13. The device of claim 8, 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.

14. The device of claim 13, wherein the plurality of security mode data structures contains information about which security modes of operation are being used by which mobile devices.

15. (Currently Amended) A method for 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;

wherein an administrator interface is configured to update the security mode stored in the policy data store and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated security mode.

16-17. (Cancelled).

18. The method of claim 15, further comprising the step of receiving an indication that the device has received and entered into the sent security mode of operation.

19. The method of claim 15, wherein the sending of the stored security mode of operation forces use of Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

20-21. (Cancelled)

22. (Currently Amended) 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;

wherein an administrator interface is configured to update the security mode and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated security mode.

23. 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.

24. 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.

25. (NEW) A non-transitory computer-readable media programmed with instructions for commanding one or more data processors to execute a method for establishing a security-related mode of operation for computing devices, 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;

wherein an administrator interface is configured to update the security mode stored in the policy data store and for communicating security modes of operation to the computing device, wherein the administrator interface provides an indication that the computing device has entered into a security mode that is compliant with the updated security mode.

Interview Summary

The Examiner contacted applicant's rep. on March 30, 2011 concerning a proposed claim amendment to overcome the prior art. The Examiner proposed adding the subject matter contained in dependent claim 6 to each independent claim. Applicant's rep. agreed to the proposed amendment after consultation with their clients. The amendment is captured above in an Examiner 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, Nathan Flynn 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.

/BRYAN WRIGHT/	/Gilberto Barron Jr./
Examiner, Art Unit 2431	Supervisory Patent Examiner, Art Unit 2432

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.
11/065,901	08/30/2011	8010989	555255012798	4175

89441 7590 08/10/2011

Jones Day (RIM) - 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 886 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, Peterborough, CANADA;
Michael S. Brown, Waterloo, CANADA;
Michael G. Kirkup, Waterloo, CANADA;
Herbert A. Little, Waterloo, CANADA;
David Victor MacFariane, Waterloo, CANADA;
Ian M. Robertson, Waterloo, CANADA;

IR103 (Rev. 10/09)