Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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 BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 112117

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

SecurityProfiling, LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	John Bignaut		
Title	Member - SecurityProfiling, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	THOMAS DONALD FORTENBERRY
Attorney Docket Number:	SP1P0012
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**730**

Electronic Acknowledgement Receipt	
EFS ID:	20264508
Application Number:	14499230
International Application Number:	
Confirmation Number:	9215
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	112117
Filer:	THOMAS DONALD FORTENBERRY
Filer Authorized By:	
Attorney Docket Number:	SP1P0012
Receipt Date:	28-SEP-2014
Filing Date:	
Time Stamp:	22:52:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$730
RAM confirmation Number	7475
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Application Data Sheet	20140928_SP1P0012_FILED_ADS.pdf	1561421 54271480c07d10d9c9fa10b4fc46fed77e011775	no	7
Warnings:					
Information:					
2		20140928_SP1P0012_FILED_Application.pdf	211125 160eb37bb142381e6c1ee7af1cf3e85a6b4f16c8	yes	49
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	47	
	Claims		48	48	
	Abstract		49	49	
Warnings:					
Information:					
3	Oath or Declaration filed	20140928_SP1P0012_FILED_Combined_Dec_and_Assign_Bligaut.pdf	70337 db574e2bfdb4306c519676697a66731ff28751ea	no	1
Warnings:					
Information:					
4	Oath or Declaration filed	20140928_SP1P0012_FILED_Declaration_Oliphant.pdf	67212 948766685ea901d03030eafa7151e7e9fe98ba2d7	no	1
Warnings:					
Information:					
5	Drawings-only black and white line drawings	20140928_SP1P0012_FILED_Figures.pdf	530013 280329e0a9702b40e7ae5993cc757eb95ebe0d2b	no	12
Warnings:					
Information:					
6	Petition for Glossary Pilot	20140928_SP1P0012_FILED_Petition_to_Make_Special.pdf	138105 aedcc2863696c22638410718 7b8c1a373b768dd4	no	1
Warnings:					
Information:					
7	Power of Attorney	20140928_SP1P0012_FILED_POA.pdf	77187 660a046f56ab8bcf2266216e1e7bbc1d2854839d	no	1
Warnings:					
Information:					

8	Fee Worksheet (SB06)	fee-info.pdf	32838 50cfdb645521372e6764ebafdbc03e58c35a7eb4	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	2688238	

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/AIA/14 (12-13)
Approved for use through 01/31/2014. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P0012
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

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

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Brett	M.	Oliphant	

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

City	Plano	State/Province	TX	Country of Residence	US

Mailing Address of Inventor:

Address 1	SecurityProfiling, LLC
Address 2	1919 S Shiloh Rd.

City	Garland	State/Province	TX
Postal Code	75042	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	P.	Blignaut	

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

City	West Lafayette	State/Province	IN	Country of Residence	US

Mailing Address of Inventor:

Address 1	SecurityProfiling, LLC
Address 2	1919 S Shiloh Rd.

City	Garland	State/Province	TX
Postal Code	75042	Country	US

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

Correspondence Information:

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P0012
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

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

Customer Number	112117		
Email Address	tom@tflawoffices.com	Add Email	Remove Email

Application Information:

Title of the Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION		
Attorney Docket Number	SP1P0012	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	12	**Suggested Figure for Publication (if any)**	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

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

Representative Information:

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

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	112117		

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P0012
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	14138014	2013-12-21
Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14138014	Continuation of	10882852	2004-07-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10882852	Claims benefit of provisional	60484085	2003-07-01

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

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P0012
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P0012
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(•) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :	

If the Applicant is an Organization check here. [X]

Organization Name	SecurityProfiling, LLC		
Mailing Address Information:			
Address 1	1919 S Shiloh Rd.		
Address 2			
City	Garland	**State/Province**	TX
Country [i]	US	Postal Code	75042
Phone Number		Fax Number	
Email Address			

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

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. [ ]

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P0012
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Thomas D. Fortenberry/			Date (YYYY-MM-DD)	2014-09-28
First Name	Thomas	Last Name	Fortenberry	Registration Number	56537

Additional Signature may be generated within this form by selecting the Add button. Add

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ForcePoint LLC
EX-1009
Page013

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part (for the purposes of providing a glossary in accordance with the Glossary Pilot Program) of U.S. App. No.: 14/138,014 filed December 21, 2013 which, in turn, is a continuation of U.S. App. No.: 10/882,852 filed July 1, 2004 which, in turn, claims priority to U.S. App. No.: 60/484,085 filed July 1, 2003, which are all incorporated herein by reference in their entirety for all purposes.

FIELD OF THE INVENTION

[0002] The present invention relates to computer systems, and more particularly to management of security of computing and network devices that are connected to other such devices.

SUMMARY

[0003] A system, method, and computer program product are provided for a database associating a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities. Each of the device vulnerabilities is associated with at least one remediation technique. Each remediation technique associated with a particular device vulnerability remediates that particular vulnerability. Further, each remediation technique has a remediation type are selected from the type group consisting of patch, policy setting, and configuration option. Still yet, a first one of the device vulnerabilities is associated with at least two alternative remediation techniques.

ForcePoint LLC
EX-1009
Page014

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a block diagram of a networked system of computers in one embodiment of the present invention.

[0005] FIG. 2 is a block diagram showing components of several computing devices in the system of FIG. 1.

[0006] FIGS. 3 and 4 trace signals that travel through the system of FIGS. 1 and 2 and the present invention is applied to them.

[0007] FIG. 5A is a flow chart of a filtering proxy method according to one embodiment of the present invention.

[0008] FIG. 5B and 6 illustrate a platform, in accordance with possible embodiments.

[0009] FIG. 7 illustrates an intelligent IDS, in accordance with one embodiment.

[0010] FIG. 8 illustrates an update system, in accordance with one embodiment.

[0011] FIG. 9 shows a configured network, in accordance with one embodiment.

[0012] FIG. 10 shows policy compliance and enforcement, in accordance with one embodiment.

[0013] FIG. 11 illustrates an intelligent IPS, in accordance with one embodiment.

[0014] FIG. 12 illustrates an SDK function call flow, in accordance with one embodiment.

DETAILED DESCRIPTION

GLOSSARY

[0015] data warehouse = a component that contains vulnerabilities and updates for devices that operate on at least one network

ForcePoint LLC
EX-1009
Page015

[0016] NOC server = network operations center server that periodically synchronize latest vulnerability and update data with other servers.

[0017] SDK = software development kit that allows programmers to develop security applications that access data collected in a database

[0018] CM application = change management application that controls documentation and logging of change.

[0019] For the purpose of promoting an understanding of the principles of the present invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will, nevertheless, be understood that no limitation of the scope of the invention is thereby intended; any alterations and further modifications of the described or illustrated embodiments, and any further applications of the principles of the invention as illustrated therein are contemplated as would normally occur to one skilled in the art to which the invention relates.

[0020] Generally, the present invention in one embodiment operates in the context of a network as shown in FIG. 1. System 100 includes a vulnerability and remediation database 110 connected by Internet 120 to subnet 130. In this exemplary embodiment, firewall 131 serves as the gateway between Internet 120 and the rest of subnet 130. Router 133 directs connections between computers 137 and each other and other devices on Internet 120. Server 135 collects certain information and provides certain data services that will be discussed in further detail herein.

[0021] In particular, security server 135 includes processor 142, and memory 144 encoded with programming instructions executable by processor 142 to perform several important security-related functions. For example, security server 135 collects data from devices 131, 133, 137, and 139, including the software installed on those devices, their configuration and policy settings, and patches that have been installed. Security server 135 also obtains from vulnerability and remediation database 110 a regularly updated list of security vulnerabilities in software for a wide variety of operating systems, and even in the operating systems themselves. Security server 135 also downloads a regularly updated list of remediation techniques that can be applied to

ForcePoint LLC
EX-1009
Page016

protect a device from damage due to those vulnerabilities. In one embodiment, each vulnerability in remediation database 110 is identified by a vulnerability identifier, and the vulnerability identifier can be used to retrieve remediation information from database 110 (and from database 146, discussed below in relation to FIG. 2).

[0022] In one embodiment, computers 137 and 139 each comprise a processor 152, 162, memory 154, 164, and storage 156, 166. Computer 137 executes a client-side program (stored in storage 156, loaded into memory 154, and executed by processor 152) that maintains an up-to-date collection of information regarding the operating system, service pack (if applicable), software, and patches installed on computer 137, and the policies and configuration data (including configuration files, and elements that may be contained in files, such as *.ini and *.conf files and registry information, for example), and communicates that information on a substantially real-time basis to security server 135. In an alternative embodiment, the collection of information is not retained on computer 137, but is only communicated once to security server 135, then is updated in real time as changes to that collection occur.

[0023] Computer 139 stores, loads, and executes a similar software program that communicates configuration information pertaining to computer 139 to security server 135, also substantially in real time. Changes to the configuration registry in computer 139 are monitored, and selected changes are communicated to security server 135 so that relevant information is always available. Security server 135 may connect directly to and request software installation status and configuration information from firewall 131 and router 133, for embodiments wherein firewall 131 and router 133 do not have a software program executing on them to communicate this information directly.

[0024] This collection of information is made available at security server 135, and combined with the vulnerability and remediation data from source 110. The advanced functionality of system 100 is thereby enabled as discussed further herein.

[0025] Turning to FIG. 2, one sees additional details and components of the devices in subnet 130. Computers 137 and 139 are traditional client or server machines, each having a processor 152, 162, memory 154, 164, and storage 156, 166. Firewall 131 and router 133 also have processors 172, 182 and storage 174, 184, respectively, as is known in the art. In this embodiment, devices 137 and 139 each execute a client-side program that continuously monitors

ForcePoint LLC
EX-1009
Page017

the software installation and configuration status for that device. Changes to that status are communicated in substantially real time to security server 135, which continuously maintains the information in database 146. Security server 135 connects directly to firewall 131 and router 133 to obtain software installation and configuration status for those devices in the absence of a client-side program running thereon.

[0026] Processors 142, 152, 162 may each be comprised of one or more components configured as a single unit. Alternatively, when of a multi-component form, processor 142, 152, 162 may each have one or more components located remotely relative to the others. One or more components of processor 142, 152, 162 may be of the electronic variety defining digital circuitry, analog circuitry, or both. In one embodiment, processor 142, 152, 162 are of a conventional, integrated circuit microprocessor arrangement, such as one or more PENTIUM 4 or XEON processors from INTEL Corporation of 2200 Mission College Boulevard, Santa Clara, Calif., 95052, USA, or ATHLON XP processors from Advanced Micro Devices, One AMD Place, Sunnyvale, Calif., 94088, USA.

[0027] Memories 144, 154, 164 may include one or more types of solid-state electronic memory, magnetic memory, or optical memory, just to name a few. By way of non-limiting example, memory 40b may include solid-state electronic Random Access Memory (RAM), Sequentially Accessible Memory (SAM) (such as the First-In, First-Out (FIFO) variety or the Last-In First-Out (LIFO) variety), Programmable Read Only Memory (PROM), Electrically Programmable Read Only Memory (EPROM), or Electrically Erasable Programmable Read Only Memory (EEPROM); an optical disc memory (such as a DVD or CD ROM); a magnetically encoded hard drive, floppy disk, tape, or cartridge media; or a combination of any of these memory types. Also, memories 144, 154, 164 may be volatile, nonvolatile, or a hybrid combination of volatile and nonvolatile varieties.

[0028] In this exemplary embodiment, storage 146, 156, 166 comprises one or more of the memory types just given for memories 144, 154, 164, preferably selected from the non-volatile types.

[0029] This collection of information is used by system 100 in a wide variety of ways. With reference to FIG. 3, assume for example that a connection request 211 arrives at firewall 131 requesting that data be transferred to computer 137. The payload of request 211 is, in this

ForcePoint LLC
EX-1009
Page018

example, a probe request for a worm that takes advantage of a particular security vulnerability in a certain computer operating system. Based on characteristics of the connection request 211, firewall 131 sends a query 213 to security server 135. Query 213 includes information that security server 135 uses to determine (1) the intended destination of connection request 211, and (2) some characterization of the payload of connection request 211, such as a vulnerability identifier. Security server 135 uses this information to determine whether connection request 211 is attempting to take advantage of a particular known vulnerability of destination machine 137, and uses information from database 146 (see FIG. 2) to determine whether the destination computer 137 has the vulnerable software installed, and whether the vulnerability has been patched on computer 137, or whether computer 137 has been configured so as to be invulnerable to a particular attack.

[0030] Security server 135 sends result signal 217 back to firewall 131 with an indication of whether the connection request should be granted or rejected. If it is to be granted, firewall 131 passes the request to router 133 as request 219, and router 133 relays the request as request 221 to computer 137, as is understood in the art. If, on the other hand, signal 217 indicates that connection request 211 is to be rejected, firewall 133 drops or rejects the connection request 211 as is understood in the art.

[0031] Analogous operation can protect computers within subnet 130 from compromised devices within subnet 130 as well. For example, FIG. 4 illustrates subnet 130 with computer 137 compromised. Under the control of a virus or worm, for example, computer 137 sends connection attempt 231 to router 133 in an attempt to probe or take advantage of a potential vulnerability in computer 139. On receiving connection request 231, router 133 sends relevant information about request 231 in a query 233 to security server 135. Similarly to the operation discussed above in relation to FIG. 3, security server 135 determines whether connection request 231 poses any threat, and in particular any threat to software on computer 139. If so, security server 135 determines whether the vulnerability has been patched, and if not, it determines whether computer 139 has been otherwise configured to avoid damage due to that vulnerability. Security server 135 replies with signal 235 to query 233 with that answer. Router 133 uses response 235 to determine whether to allow the connection attempt.

ForcePoint LLC
EX-1009
Page019

[0032] In some embodiments, upon a determination by security server 135 that a connection attempt or other attack has occurred against a computer that is vulnerable (based on its current software, patch, policy, and configuration status), security server 135 selects one or more remediation techniques from database 146 that remediate the particular vulnerability. Based on a prioritization previously selected by an administrator or the system designer, the remediation technique(s) are applied (1) to the machine that was attacked, (2) to all devices subject to the same vulnerability (based on their real-time software, patch, policy, and configuration status), or (3) to all devices to which the selected remediation can be applied.

[0033] In various embodiments, remediation techniques include the closing of open ports on the device; installation of a patch that is known to correct the vulnerability; changing the device's configuration; stopping, disabling, or removing services; setting or modifying policies; and the like. Furthermore, in various embodiments, events and actions are logged (preferably in a non-volatile medium) for later analysis and review by system administrators. In these embodiments, the log also stores information describing whether the target device was vulnerable to the attack.

[0034] A real-time status database according to the present invention has many other applications as well. In some embodiments, the database 146 is made available to an administrative console running on security server 135 or other administrative terminal. When a vulnerability is newly discovered in software that exists in subnet 130, administrators can immediately see whether any devices in subnet 130 are vulnerable to it, and if so, which ones. If a means of remediation of the vulnerability is known, the remediation can be selectively applied to only those devices subject to the vulnerability.

[0035] In some embodiments, the database 146 is integrated into another device, such as firewall 131 or router 133, or an individual device on the network. While some of these embodiments might avoid some failures due to network instability, they substantially increase the complexity of the device itself. For this reason, as well as the complexity of maintaining security database functions when integrated with other functions, the network-attached device embodiment described above in relation to FIGS. 1-4 is one possible embodiment.

[0036] In one embodiment, a software development kit (SDK) allows programmers to develop security applications that access the data collected in database 146. The applications developed with the SDK access information using a defined application programming interface

ForcePoint LLC
EX-1009
Page020

(API) to retrieve vulnerability, remediation, and device status information available to the system. The applications then make security-related determinations and are enabled to take certain actions based on the available data.

[0037] In these exemplary systems, "configuration information" for each device may take the form of initialization files (often named *.ini or *.conf), configuration registry (such as, the Windows Registry on Microsoft WINDOWS operating systems), or configuration data held in volatile or non-volatile memory. Such configuration information often determines what and how data is accepted from other devices, sent to other devices, processed, stored, or otherwise handled, and in many cases determines what routines and sub-routines are executed in a particular application or operating system.

[0038] In one embodiment, security information management system is provided, wherein a database of potential vulnerabilities is maintained, along with data describing remediation techniques (patches, policy settings, and configuration options) available to protect against them. At least one vulnerability is associated in the database with multiple available remediation techniques. In one embodiment, the system presents a user with the list of remediation techniques available to protect against a known vulnerability, accepts the user's selection from the list, and executes the selected technique. In other embodiments, the system uses a predetermined prioritization schedule to automatically select among the available remediation techniques, then automatically executes the selected technique.

[0039] One embodiment of the present invention is a database of information about a plurality of devices, updated in real-time and used by an application to make a security-related decision. The database stores data indicating the installed operating system(s), installed software, patches that have been applied, system policies that are in place, and configuration information for each device. The database answers queries by one or more devices or applications attached by a network to facilitate security-related decision making. In one form of this embodiment, a firewall or router handles a connection request or maintenance of a connection based on the configuration information stored in the database that relates to one or both of the devices involved in the transmission.

[0040] In one embodiment, database 146 includes vulnerability and remediation information such that, for at least one vulnerability, multiple methods of remediating the vulnerability are

ForcePoint LLC
EX-1009
Page021

specified. When the system has occasion to implement or offer remediation of a vulnerability, all known alternatives are presented that are relevant to the device or machine's particular configuration or setup. For example, when a vulnerability of a device is presented to an administrator, the administrator is given a choice among the plurality of remediation options to remediate the vulnerability. In some embodiments, the administrator can select a preferred type of remediation that will be applied if available and a fallback type. For example, an administrator may select application of a policy setting over installation of a software patch, so that the risk of disruption of critical business systems is minimized.

[0041] In other embodiments, an administrator or other user is presented with a set of user interface elements that identify multiple options for remediating and identifying the vulnerability. The administrator or user selects the method to be used, and that remediation is applied to the vulnerable device(s).

[0042] FIG. 5A is a flow chart of a filtering proxy method according to one embodiment of the present invention.

[0043] In use, a database maintains security status information on each device in a network, based on whether the device's operating system, software, and patches are installed and configured to meet a baseline level of security. A network gateway proxy blocks connection attempts from devices for which the database indicates a substandard security status, but allows connections from other devices to pass normally. The database is preferably updated on a substantially real-time basis by client-side software run by each device in the network.

[0044] Another form of the present embodiment includes a connection proxy that filters connections originating within the network. In particular, one embodiment employs a proxy that denies connection attempts originating with devices in the network when the originating device has a status, reflected in the database, that fails to meet predetermined security characteristics in terms of installed operating system and software, patch levels, and system policy and configuration registry information.

[0045] In this embodiment, router 133 serves as a connection proxy for devices and subnet 130, as will be understood by those skilled in the art. In addition to basic proxy functionality, however, router 133 accesses database 146 on security server 135 via the SDK at each connection attempt. If, for example, device 137 attempts to connect to any device where the

ForcePoint LLC
EX-1009
Page022

connection must pass through the proxy server (router 133 in this example), such as a device on Internet 120, router 133 checks the security status of device 137 in database 146, using the real-time status therein to determine whether device 137 complies with one or more predetermined security policies. If it does, router 133 allows the connection to be made. If it does not, router 133 prevents the connection, preferably redirecting the connection to a diagnostic page that explains why the connection is not being made.

[0046] This system is illustrated by method 200 in FIG. 5A. Method 200 begins with start point 201. The proxy (router 133 in the above example) receives a connection request at block 203, then retrieves the security status of the source device at block 205. This preferably uses the real-time updated status information from database 146 (see FIG. 2) at decision block 207. If the security status indicates that the source device complies with the predetermined security policy, the proxy allows the connection at block 209. If not, the proxy refuses the connection at block 211 and redirects the connection to an explanation message (such as a locally generated web page or other message source) at block 213. In either case, method 200 ends at end point 219.

[0047] In possible embodiments, the determination and decision at block 207 apply a comprehensive minimum policy set that protects other devices in subnet 130 (see FIG. 1) from viruses, trojans, worms, and other malware that might be inadvertently and/or carelessly acquired due to the requested connection.

[0048] In another embodiment, a security information management system is provided, wherein client-side devices preferably collect and monitor information describing the operating system, software, and patches installed on the device(s), as well as configuration thereof. A database of this information is maintained, along with data describing vulnerabilities of available software and associated remediation techniques available for it. The system exposes an API to support security-related decisions by other applications. For example, an intrusion detection system (IDS) accesses the database to determine whether an actual threat exists and should be (or has been) blocked.

[0049] In another form of this embodiment, client software runs on each monitored device and reports configuration information to the database, so that the database has substantially real-time-current information.

ForcePoint LLC
EX-1009
Page023

[0050] The present embodiment of the present invention advantageously acquires the real-time status information from each client using client-side software. In this manner, a resource burden of monitoring is spread among the devices being monitored, and uses far fewer network resources in the process.

[0051] In these exemplary systems, "configuration information" for each device may take the form of initialization files (often named *.ini or *.conf), configuration registry (such as the Windows Registry on Microsoft Windows operating systems), or configuration data held in volatile or non-volatile memory. Such configuration information often determines what and how data is accepted from other devices, sent to other devices, processed, stored, or otherwise handled, and in many cases determines what routines and sub-routines are executed in a particular application or operating system.

[0052] In one embodiment, a system maintains a database of vulnerabilities and associated remediation techniques. The remediation techniques include software patches, policy settings or changes, and registry settings or changes. This multi-faceted provides novel flexibility in management of security issues, and convenience for security administrators in both determining available options and selecting remediation steps for vulnerable systems.

[0053] In another embodiment of the present invention, patches, policy changes, software updates, and configuration changes are rolled out to devices on a network using a staged roll-out technique. In this technique, the change is applied to a selected device or set of devices identified by an administrator. After a predetermined amount of time passes, unless the administrator has canceled the roll-out, the change is applied to an additional group of devices on the network. Third- and fourth-tier groups may also be identified by the administrator, where implementation of the remediation or upgrade is automatically effected in subsequent stages a predetermined amount of time after the preceding stage roll-out. Thus, if no failures are noted following a more limited roll-out (on a first set of devices), then the remediation or upgrade is automatically applied to other devices. If, on the other hand, an error or failure is observed, the subsequent roll-out can be canceled so that further failures and problems are avoided.

[0054] FIG. 5B and 6 illustrate a platform, in accordance with possible embodiments.

[0055] In one possible embodiment, provided is a platform and underlying back end that includes a logic engine and vulnerability data warehouse. It may easily integrate with and enable

ForcePoint LLC
EX-1009
Page024

network security products such as IDS, scanners, or firewalls to intelligently reference and share the same vulnerability data set, and independently provide complete vulnerability remediation (patching) functionalities such as that provided by the patch management and vulnerability remediation application. Thereby, the technology may improve system accuracy and efficiencies, minimize false positives and false negatives, and provide policy compliance and enforcement capabilities.

[0056] The latest network compromises are combining qualities of viruses, worms, and denial of service attacks into new blended attacks. Additionally, blended attacks may now utilize metamorphic or polymorphic abilities to change their signatures to avoid detection. To mitigate these new risks, organizations are now deploying a multi-tiered network defense strategy comprised of a variety of network security components layered at the perimeter and to internal network machines and devices. The security components are managed separately, and possibly their data is ported into a Security Information Management System (SIMS) correlation engine.

[0057] However, network security components and correlation engines rely on signatures or anomalies, producing an ever-increasing quantity of data, including false positive, benign, and erroneous events. They also lack the intelligence to identify, reference, or remediate the vulnerabilities targeted by the attack. Furthermore, the time and cost to acquire, manage, and maintain these numerous network security components is overwhelming the end user. Therefore, more sophisticated technology is provided to resolve these performance and management issues.

[0058] In one embodiment, technology may be provided that addresses these requirements by making each security component smarter and provides managers with remote remediation options. Thereby, improving system performance and streamlining management processes.

[0059] In one embodiment, an intelligent integration platform and SDK are provided to meet the above requirements.

[0060] In one embodiment, security products are enhanced and system intelligence may be provided. The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats.

[0061] One embodiment cross-references the threat's identifier with the target's configuration. The threat's CVE ID, or other identifier, and the destination IP address are fed

ForcePoint LLC
EX-1009
Page025

into the logic engine where it cross-references the threat with the machine's existing OS, application, and patch configuration profile. An answer is returned accurately indicating if the machine is vulnerable.

[0062] In one embodiment, network vulnerabilities are identified. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

[0063] One embodiment proactively remediates the vulnerability. Once a vulnerability is identified, a remediation function may be provided that may remotely and automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

[0064] Examples of Anti-Vulnerability applications that may be integrated into network security products for enterprise and small office home office (SOHO) networks when integrated with one embodiment, via the SDK, will be described.

[0065] In one embodiment, update or patch deployment are provided, which remotely remediate network vulnerabilities and provide policy compliance and enforcement capabilities. And, for the consumer market, it may additionally support non-security related updates such as application version, performance, and bug-fix upgrades.

[0066] In one embodiment, an IDS may be provided that accurately determines if the targeted machine is actually vulnerable to an attack; virtually eliminates false positives and false negatives; and adds vulnerability remediation and policy compliance and enforcement functionalities.

[0067] In one embodiment, a scanner may be provided that virtually eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities.

[0068] In one embodiment, a firewall may be provided that virtually eliminates false positive and false negatives, preventing the security system from denying valid traffic to the organization – self-inflicted denial of service attacks - and adds vulnerability remediation, and policy compliance and enforcement functionalities.

[0069] In one embodiment, vulnerability management may be provided, as set forth above.

ForcePoint LLC
EX-1009
Page026

[0070] In one embodiment, multiple products are provided including an IDS, scanner, and firewall. Each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats.

[0071] In one embodiment, change management may be provided, which may automatically create a change request in the system, specifying what update/patch is applicable to what system or groups of systems by vulnerability. After approval of the request, they may automatically deploy and install the update/patch. Finally, they may also verify correct operation after installation and automatically provide all necessary documentation and logging required.

[0072] Lastly, the platform may also provide product upgrades and signature updates to each of these various security products.

[0073] The platform is comprised of the following software components: SDK, client agent, logic engine, and data warehouse stored on a dedicated on-site server. Network operations center (NOC) Servers periodically synchronize the customers' servers with the latest vulnerability and update data. See FIG. 5B.

[0074] The same client agent and on-site server support all security applications that are integrated onto the platform, thereby providing the added anti-vulnerability functionalities presented in the previous section.

[0075] There are two system requirements: TCP/IP connectivity, and supported network machines and devices. In one embodiment, platforms supported are set forth below in Table 1.

Table 1

All Windows Operating Systems and their applications
All UNIX variants
Cisco routers and firewalls
Toshiba network devices
Netgear network devices
Linksys network devices, including wireless access points

ForcePoint LLC
EX-1009
Page027

[0076] Platform support is scalable to any network size or architecture; consumer, small office home office (SOHO), enterprise, and distributed networks.

[0077] In one embodiment, technology may be provided that includes a backend platform that includes a logic engine and vulnerability data warehouse. It may easily integrate with and enable network security products such as IDS, scanners, or firewalls to intelligently reference and share the same vulnerability data set, and independently provide complete vulnerability remediation (patching) functionalities such as that provided by the patch management and vulnerability remediation application, update application and the intelligent IDS. Thereby, the technology may improve system accuracy and efficiencies, minimize false positives and false negatives, and provide policy compliance and enforcement capabilities.

[0078] As shown in FIG. 5B, the technology may meet market requirements, presented in the next section.

[0079] For example, networks are probed at an ever-increasing frequency for vulnerabilities, which may be exploited with compromise attacks. To protect the network, administrators have traditionally set up perimeter defense strategies.

[0080] These strategies generally call for network managers to lock down core servers, and monitor/scan/filter all incoming and outgoing traffic at the network perimeter with several network security products such as antivirus and firewalls to identify and attempt to neutralize hackers and malicious code. In the past, these strategies worked well, however new threats are becoming more complex.

[0081] The latest malicious code may combine qualities of viruses, worms, and direct compromise attacks into new blended attacks. Virus payloads are becoming more complex and by using metamorphic or polymorphic abilities, viruses are able to change their signatures to avoid the fingerprint-type filtering that most applications employ.

[0082] To mitigate these new risks, organizations deploy a multi-tiered network defense strategy comprised of a variety of additional network security products layered at the perimeter and to internal network machines and devices. Such network security products include antivirus, firewall, scanners, and network and host based intrusion detection systems.

ForcePoint LLC
EX-1009
Page028

[0083] Each of these systems is based on specific signatures, rules, or anomalies of each attack and their variants, and do not identify and remediate the specific network vulnerabilities the attack is targeting. So each attack, and its variants, must be identified and analyzed, a signature prepared, then finally deployed to each point product on each customer's network. This process is uncoordinated among multiple disparate systems, and creates an ever-increasing number of signatures producing more and more attack alerts requiring immediate attention – many of which are erroneous. The security components are managed separately, and possibly their data is ported into a security information management system (SIMS) correlation engine.

[0084] Additionally, to proactively remediate the vulnerabilities the malicious code is targeting, administrators quickly and diligently update or "patch" each network machine and device, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives may require higher standards of network security and integrity to protect consumer privacy, and they are documented with change tracking and audit trail reports.

[0085] Therefore, it is increasingly difficult and costly to effectively mitigate new threats and manage numerous systems — particularly in an environment of rising security standards and policy compliance requirements.

[0086] Thus, the multi-tiered network defense strategy is falling short primarily for four reasons. First, there is an inability of multi-tiered network security products to communicate and share information necessary to mitigate blended threats, and minimize false positives and false negatives. The vulnerabilities targeted by malicious code are not accurately identified nor proactively remediated. The associated excessive aggregate cost of ownership of multiple systems. The excessive administrative burden and cost of managing and maintaining multiple systems.

[0087] Hence, there is a need to integrate systems, share information intelligently to better defend against blended threats, reduce management and cost requirements, and automate vulnerability identification and remediation functionalities, as presented in the high-level requirements.

ForcePoint LLC
EX-1009
Page029

[0088] In one embodiment, technology is provided to meet the following market requirements: integrate network security products to share information; provide system intelligence; and remediate network vulnerabilities.

[0089] In one embodiment, technology may integrate with and enable network security products to intelligently reference and share information from the same vulnerability data set, provide vulnerability identification and remediation functionalities, and efficiently meet policy compliance and enforcement requirements.

[0090] In one embodiment, the platform is a complimentary network security technology. When integrated into the defense strategy, it adds intelligence that more accurately and efficiently mitigates blended threats and offloads the time-consuming functions that burden network administrators.

[0091] In one embodiment, the platform enables network security products to share information via its proprietary logic engine to automatically cross-reference the threat identifier with the targeted machine's configuration to determine if it is actually vulnerable to that threat. Previously separate and uncoordinated processes are now more intelligent and automated, resulting in improved system accuracy and efficiency. Therefore the need to layer more and more point products and add a SIMS is reduced, in-turn decreasing the amount of data – particularly erroneous data – to manage. Subsequently, the costs to acquire, operate, and manage the additional multiple point products, and the need to implement a SIMS, are also reduced.

[0092] In one embodiment, the platform may also remotely and proactively remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented.

[0093] In one embodiment, the present technology fulfills market requirements noted in the previous section. For example, it may integrate network security products and provides system intelligence. The same vulnerability data warehouse information is shared with all products so that more intelligent actions may then be taken to mitigate complex threats.

ForcePoint LLC
EX-1009
Page030

[0094] Still yet, it may cross-reference the threat's identifier with the target's configuration. The threat's CVE ID, or other identifier, and the destination IP address are fed into the logic engine where it cross-references the threat with the machine's existing OS, application, and patch configuration profile. An answer is returned accurately indicating if the machine is vulnerable. Thereby, minimizes erroneous, benign, and false positive data produced by each security product.

[0095] One embodiment identifies network vulnerabilities. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

[0096] One embodiment proactively remediates the vulnerability. Once a vulnerability is identified, a remediation function may be provided that may remotely and automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

[0097] Various possible benefits include blended attacks being more effectively mitigated and the overwhelming management and maintenance burden on administrators to purchase, operate, and maintain multiple network security products being reduced, while increasing productivity, reducing costs, and more effectively and efficiently meeting policy compliance and enforcement requirements.

[0098] Table 2 illustrates a plurality of end user details.

Table 2

- Supplements existing technology to better defend against blended attacks
- Intelligently accesses the vulnerability data warehouse, and remediates vulnerabilities.
- Offers policy compliance and enforcement functionality
- Vulnerabilities may be automatically remediated, verified and documented, therefore enforcing compliance.
- No additional software or hardware implementation costs

ForcePoint LLC
EX-1009
Page031

- Anti-Vulnerability functionalities may be integrated into existing product platforms.
- Reduces cost of ownership of multi network security products
- Shared vulnerability data sets and added vulnerability remediation functionalities may reduce the number of network security products needed to adequately attain defense strategy requirements.
- Reduces management and maintenance costs
- Increased accuracy of vulnerability identification, remediation and policy enforcement, and reduction of false positives, false negatives and denial of service (DoS), significantly reduces management time and costs.
- Manage more machines and devices on the network through one portal
- Vulnerability remediation and policy compliance and enforcement may be integrated with existing security network security products, and their respective interfaces.
- Minimize end user education/ absorption costs
- Anti-Vulnerability applications are transparently integrated, retaining pre-existing architecture, processes, and interfaces. Therefore, the end user experience remains the same, or improved with simplified or automated processes.
- User experience remains the same – additional time or costs to understand and execute new technologies are minimized
- Anti-Vulnerability applications may be integrated transparently and seamlessly, and the pre-existing operational processes and user interfaces are virtually unchanged.
- Supports both the enterprise and SOHO networks
- Data warehouse contains vulnerabilities and updates for many machines and devices that operate on both enterprise and SOHO networks.
- Applications presented hereinafter

ForcePoint LLC
EX-1009
Page032

[0099] Examples of applications that may be made available for enterprise and small office home office (SOHO) networks when integrated with Anti-Vulnerability technology via the SDK will now be set forth.

[00100] In one embodiment, update or patch deployment is provided. In one embodiment, a patch management and vulnerability remediation solution is provided. The technology enables products to add accurate vulnerability identification, remediation, verification, and policy compliance functions. With such technology, products may gain intelligence, accuracy and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks. And, for the consumer market, it may additionally support non-security related updates such as application version, performance, and bug-fix updates for widely distributed programs, which may optimize system performance and enhance the consumer experience.

[00101] In one embodiment, an IDS is provided. IDS products attempt to identify malicious code by signatures at both the network and host client level. While they may be able to identify malicious code by CVE ID or other identifier, and targeted machines by IP address, but they generally do not have the intelligence to determine if the any of the machines on the network are susceptible to that attack, or with finer granularity, if any machine has a specific vulnerability to that specific attack, or if the targeted vulnerability has already been patched. For example, if the malicious code has been written as a Windows based attack targeting a Windows vulnerability, is the Destination IP actually running Windows, or a UNIX variant? And, if Windows, is it vulnerable to the attack, or has it already been patched? IDS do not have the intelligence to answer these questions, and incident alerts are generated indiscriminately. Lastly, even if the targeted machine is vulnerable - it remains unremediated – an IDS does not have the capability to remediate it.

[00102] With the present embodiment, a product architect can integrate functionalities listed in the previous section to enable the IDS to access the Anti-Vulnerability logic engine and platform. It may then have the intelligence to determine if any machine on the network is susceptible to the attack, remediate the vulnerability, mitigate the attack, and verify policy compliance. Now, if no machines were susceptible to the attack, it is identified as an event but

ForcePoint LLC
EX-1009
Page033

not an incident, no further data or alert is generated, and a management response is not required. Integrated products may gain intelligence, accuracy, and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks.

[00103] In one embodiment, scanners may be provided. Vulnerability scanners assess each machine on the network for vulnerabilities, and create lists of potential vulnerabilities to the system managers. The lists commonly contain many false positives and false negatives, burdening the system and managers with inaccuracies.

[00104] With the present embodiment, a product architect can integrate functionalities listed in the previous section to enable the scanner to access the logic engine and platform, and then have the intelligence to determine if the machine has actual vulnerabilities, remediate them, and verify policy compliance. Integrated products may gain intelligence, accuracy, and efficiency, eliminated false positives and false negatives, and ensured policy compliance, thereby saving the organization time and money.

[00105] In one embodiment, a firewall may be provided. "Smart" firewalls are based in part on signatures and other similar functionalities as the IDS products described above.

[00106] With the present embodiment, the firewall can determine whether an attack is valid or a false positive, thereby preventing the security system from denying valid traffic to the organization – self-inflicted DoS attacks. Such functionalities and benefits may be available for both the enterprise and SOHO networks.

[00107] In one embodiment, vulnerability management may be provided. Vulnerability management products enable managers to set policy and identify potential network vulnerabilities. They typically do not accurately identify each vulnerability on each network machine and device, nor remediate each vulnerability, meeting policy compliance enforcement requirements.

[00108] The present embodiment offers similar functionalities and benefits as the patch deployment products described above. In short, it enables products to add accurate vulnerability identification, remediation, verification, and policy compliance and enforcement. Such functionalities and benefits are available for both the enterprise and SOHO networks.

ForcePoint LLC
EX-1009
Page034

[00109] To this end, multiple products may be provided: IDS, scanner, firewall, and vulnerability management. Each product functions as the individual products noted above. Each may be deployed and operated on the network in a multi-tiered network defense strategy. They may be disparate system, and their signatures and update deployment schedules may vary. Therefore, the probability of mitigating a new and complex threat decreases, while management requirements and cost increases.

[00110] In one embodiment, they each may communicate with the same backend data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats. It may also enable the products to add accurate vulnerability identification, remediation, verification, and policy compliance and enforcement functionalities.

[00111] In one embodiment, change management (CM) may be provided. Existing CM applications control the documentation and logging of change throughout the enterprise. These applications ensure that an organization maintains consistent records of what happened and when. Currently administrators must independently recognize that a security patch/update must be deployed to a computer or group of computers.

[00112] The user enters the request in the system, through the pipelined process of change management the request would be approved, the patch/update would be manually installed by a user, then documented in the change management software that the process has been completed. While CM software assists in documentation, very little if any assistance may be provided to identify the patches/updates needed, nor verifying correct function after the update/patch is installed.

[00113] With the current possible embodiment, change management integration may greatly streamline this process further reducing total cost of ownership, ease of use, and a higher standard of documentation. The products may then automatically create a change request in the system, specifying what update/patch is applicable to what system or groups of systems by vulnerability. After approval of the request, they may automatically deploy and install the update/patch. Finally, they may also verify correct operation after installation and automatically provide all necessary documentation and logging required.

ForcePoint LLC
EX-1009
Page035

[00114] Lastly, one possible embodiment may also provide product upgrades and signature updates to each of these various security products - including all of the technology benefits such as ensuring compliance of signature versions, logging, reporting, and verification of installation.

[00115] Thus, one possible embodiment includes an intelligent platform that may supplement any existing defense strategy. Once integrated with the technology, security products may share the same vulnerability data set to improve automation and accuracy – increasing efficiencies and minimizing false positives and false negatives. It also enables remote identification, management, and remediation of network vulnerabilities, and provides update deployment, validation, and reporting capabilities. Thereby, the technology improves network security and integrity, mitigation of blended threats, while increasing productivity, reducing total cost ownership, and more effectively and efficiently attaining policy compliance and enforcement requirements.

[00116] One embodiment provides IDS intelligence, accuracy and remote patching functions - IDS data output integrated with the aforementioned platform via the SDK. The platform's underlying backend including a logic engine and vulnerability data warehouse provides the added functions and performance.

[00117] Conventional IDS produce an ever-increasing quantity of alert data, including erroneous and false positive data. They also lack the intelligence to identify or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintaining conventional IDS is overwhelming the end user.

[00118] Therefore, a more sophisticated, intelligent technology is provided to resolve these issues. In one embodiment, an intelligent IDS is provided to meet market requirements. The alert data output from a distribution of Snort is integrated with the platform via the SDK, which may add the following functions.

[00119] In one embodiment, it cross-references the threat's identifier with the target's configuration. The CVE ID, or other identifier, and the Destination IP address are fed into the logic engine where it cross-references the threat with the machine's configuration profile.

[00120] In one embodiment, it virtually eliminates false positives and false negatives. The backend accurately determines in real time if the targeted machine is susceptible to the attack.

ForcePoint LLC
EX-1009
Page036

And, if the machine is not susceptible, it is filtered and reported back as an event and not an incident. No further data or alert is generated, and a management response is not required.

[00121] In one embodiment, it remotely remediates the vulnerability. When a machine is identified as vulnerable to an attack, an incident, a remediation function may be provided to the administrator to remotely deploy the appropriate update to the machine or device, install it, verifies the files and hashes, and document it with change tracking and audit trail reports.

[00122] Table 3 sets forth a plurality of features.

Table 3

Supports Windows and UNIX variants
Determines if targeted machine is vulnerable to an attack in real time
Filters out erroneous, benign and false positive alerts
Remotely patches targeted vulnerabilities in one click
Installs in minutes

[00123] To this end, erroneous, benign, and false positive data is filtered out, and incidents may be remotely remediated. Therefore, complex threats are more effectively and efficiently mitigated. Correspondingly, the management and maintenance burden on administrators is reduced, saving time and effort.

[00124] FIG. 7 illustrates an intelligent IDS, in accordance with one embodiment. As shown in 701, the on-site server periodically initiates communication with the NOC servers. In 702, updates are pulled from the NOC servers to the on-site server. In 703a, a sensor monitors and processes network traffic, and sends real time alert data to the on-site server where it cross-references the data with the backend. In 703b, centralized IDS console filters alerts; separating events from incidents. It also offers administrators remote patching function. In 704, agents are deployed to each client, accurately identifying which OS, apps, and updates are installed. In 705, the logic engine automatically determines which updates are needed to remediate the targeted

ForcePoint LLC
EX-1009
Page037

machine. As shown in 706, appropriate updates are remotely deployed, installed, and validated on each client.

[00125] In one embodiment, the intelligent patch management and vulnerability remediation application automatically updates computer OS and application vulnerabilities before they can be exploited by hackers and viruses.

[00126] Networks are probed at an ever-increasing frequency for vulnerabilities, which may be exploited with directed compromise attacks. To protect the network, administrators must diligently update or "patch" server and workstation vulnerabilities, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives now require higher standards of network security to protect consumer privacy and proprietary data, which must be documented with change tracking and audit trail reports. Therefore, fully automated technology is provided to resolve these issues.

[00127] In one embodiment, a intelligent application called SysUpdate — the first technology to fully automate the updating and reporting processes, as described below.

[00128] In terms of function, one possible embodiment automatically researches updates. In collaboration with software development companies, it receives updates and their respective compatibility and installation guidelines, which are thoroughly reviewed and tested in a lab for system compatibility and stability. One embodiment automatically and securely downloads, and archives, all updates. Once the updates and guidelines are thoroughly reviewed and tested, they are automatically downloaded to each customer's on-site server, verified with MD5 hashes, and archived in a self-populating patch repository database.

[00129] One possible embodiment automatically determines the update and dependency requirements for all computers on a network, based on their individual operating systems, applications, and previously installed updates. The logic engine automatically matches the tested updates and their guidelines across each computer's configuration profile.

[00130] One possible embodiment remotely, securely, and automatically deploys updates to each computer and device. Updates may be tested on a test group, and then queued for release to each computer on the network, consistently in accordance with the policy determined by the network administrator.

ForcePoint LLC
EX-1009
Page038

[00131] One possible embodiment automatically verifies the updates are installed and running correctly. Each computer's client agent installs the updates, and verifies the files and hashes.

[00132] One possible embodiment automatically generates change tracking and audit trail reports. Change tracking and audit trail reports may be selected and printed from the management console reporting modules. Additionally, application license audit reports may be generated, which lists software installed on each machine, by license key.

[00133] Table 4 illustrates possible features in one embodiment.

Table 4

Supports Windows, UNIX variants, and network devices
Supports non-Microsoft applications
Logic engine provides system intelligence
Files verified with SHA1 or MD5 hashes
MMC snap-in console with Crystal Reports
AES encryption

[00134] FIG. 8 illustrates an update system, in accordance with one embodiment.

As shown in 801, the on-site server periodically initiates communication with the off-site NOC servers. In 802, updates are pulled from the NOC servers to the on-site server. In 803, the centralized MMC snap-in console offers flexible security policy options and comprehensive reporting capabilities. In 804. agents accurately identifies OS, apps, and updates installed on each client by file versions and hashes. In 805, logic engine automatically determines which updates are needed on each client, taking into account OS, app, and update dependencies. In 806, appropriate updates are automatically deployed, installed, and validated on each client.

[00135] In one embodiment, a secure computer log management application is provided with fully automated archiving, querying, and reporting options.

ForcePoint LLC
EX-1009
Page039

[00136] Best practice directives and government compliancy regulations now require administrators to archive log events over an extended period of time, and extensively document log and audit trail reports. With existing tools, these are time-consuming processes. Furthermore, existing tools transfer logs in clear text and are subject to malicious manipulation, and logs may be lost since few utilize guaranteed delivery protocols. Therefore, the integrity and security of the log data is not assured. In the event of an internal or external compromise, logs may be deleted, manipulated, or the network flooded with decoy log data.

[00137] The present possible embodiment automatically and continuously transfers logs from each computer into a self-configuring, self-populating, maintenance-free database where they may be archived for years on end. The transfer process utilizes AES encryption for authentication between the client and server, and a guarantee delivery protocol — ensuring no data is compromised or lost. Flexible cross-correlation queries may be run from a single, remote viewer console, and the data is then automatically formatted into reports.

[00138] In one embodiment, cross-correlation query type descriptions are provided. Such embodiment may provide the following three flexible cross-correlation queries in Table 5, which provide increasing detail and breadth of filtering/sorting capabilities, respectively.

Table 5

General Queries – This is the default query. It filters or sorts the logs of any one computer, by any one of the three log types.

Specific Queries – Detailed queries across all machines, and all log types.

Advanced Queries – Query across any combination of machines, by any combination of sources, events, and log types, over any period of time.

[00139] In one embodiment, features shown in Table 6 may be provided.

Table 6

ForcePoint LLC
EX-1009
Page040

- Continuously pulls all logs into a central database, which may be archived for years on end
- AES encryption and a guarantee delivery protocol ensure logs are not compromised or lost
- Queries may be across any computer, for any log type, over any time frame
- Automatically generates event log reports — ideal for documenting audit and compliance requirements
- Easy download installation

[00140] In one embodiment, automated reports may be provided. Query data is automatically formatted into professional reports Also, a separate reporting interface is available to generate general, machine, and user statistics. The present embodiment quickly and easily fulfills best practice and government compliance requirements for log event archiving and reporting.

[00141] FIG. 9 shows a configured network, in accordance with one embodiment.

[00142] As shown in 901, the server component automatically configures the application, and the database and communicates with the client agents. In 902, client agents are deployed, which then identifies, manages, and continuously transfers all logs to the server. In 903, all client log data may be automatically archived the self-populating database, for years on end. In 904, from the centralized viewer, general, specific, or advanced cross-correlation queries may be run. See Table 7. Query and statistics data is automatically formatted into professional reports to easily document audit and compliance requirements.

Table 7

Filter/Sort By:	**General**	**Specific**	**Advanced**

ForcePoint LLC
EX-1009
Page041

# of Computers	Any One	Any One	Any
# of Log Types	Any One	All	Any
Period of Time	Last or All	Last or All	Any
# of Event Detail Fields *	By ID Only	Any One	Any

* Defined as Time/Date Written, UserID, ComputerID, EventID, Source, Type, and Category

[00143] One possible embodiment provides best practice security policy templates to proactively and remotely manage and enforce enterprise security compliance policies.

[00144] Best practice and government compliance directives require higher standards of network security to protect consumer privacy and proprietary data, which must be consistently enforced, and documented with change tracking and audit trail reports for compliance verification. Therefore, a fully automated technology is provided to resolve these issues.

[00145] One embodiment offers an intelligent application to manage and enforce security policies — the first technology to fully automate the policy configuration, enforcement, and reporting processes, as described below.

[00146] In one embodiment, centralized, remote management is provided. The policy compliance and enforcement module is managed via the centralized management console - in MMC format, and automates the deployment, assessment, and enforcement of the policy chosen.

[00147] One embodiment provides standardized policies selected from many standardized policy templates recommended by NSA, SANS, US Navy, and ISO 17799, or custom policy options to formulate policies that meet the individual needs of any organization.

[00148] One possible embodiment automatically determines out-of-compliance parameters for all computers and devices on a network. Based on each client's individual policy parameter settings and configuration profile, the system's logic engine automatically reports back each client's out-of-compliance parameters.

[00149] In one embodiment, it remotely, securely, and automatically enforces policy to each computer or device. Policy changes may be automatically enforced to each computer or device

ForcePoint LLC
EX-1009
Page042

individually, or by group, consistently in accordance with the policy selected by the network administrator. Policy configuration profiles are transmitted between client agent and server in an AES encrypted format for security and privacy. Policy options may be rolled back with one-click.

[00150] Automatically generates change tracking and audit trail reports. Change tracking and audit trail reports may be selected and printed from the Management Console's Reporting Center. Table 8 sets forth some possible features.

Table 8

Supports Windows, UNIX variants, and network devices
Supports NSA, SANS, Navy, ISO 17799 and other standardized policies
Logic engine provides system intelligence
One-click policy rollback
Automatically generates change tracking and audit trail reports

[00151] FIG. 10 shows policy compliance and enforcement, in accordance with one embodiment.

[00152] As shown in 1001, the on-site server periodically initiates communication with the off-site NOC servers. In 1002, templates, rules, and updates are pulled from the NOC servers to the on-site server. In 1003, a centralized management console offers flexible security policy templates, options, and comprehensive reporting capabilities. In 1004, agents are automatically deployed to each client, accurately identifying which policy parameters, OS, apps, and updates are applied or installed. In 1005, a logic engine automatically determines which clients are out of compliance. In 1006, appropriate policy changes are automatically enforced on each client.

[00153] In one embodiment an intelligent IPS may be provided that provides intelligence, accuracy, real-time prevention, and remote patching functions. In one embodiment, it accurately identifies and prevents malicious code from reaching their destination at the in-line IPS Sensor. Thereafter, a security officer may remotely patch the targeted vulnerability.

ForcePoint LLC
EX-1009
Page043

[00154] Conventional IDS/IPS produce an ever-increasing quantity of alert data, including erroneous and false positive data. They also lack the intelligence to identify or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintaining conventional IPS is overwhelming the end user.

[00155] Therefore, a more sophisticated, intelligent technology is provided to resolve these issues, by offering an intelligent IPS to meet market requirements. The alert data output from a standard distribution of Snort is integrated with the platform via the SDK which accurately identifies attacks, and the attack is terminated at the in-line sensor – as described in the following functions.

[00156] One embodiment cross-references the threat's identifier with the target's configuration. The in-line Sensor monitors and processes traffic and sends alert data to the on-site server where its logic engine queries the backend in real-time to determine if the destination IP is vulnerable to the attack.

[00157] One possible embodiment provides enhanced flex response. If the destination IP is vulnerable to the attack, the in-line Sensor is commanded to immediately drop the exploit packets – preventing the attack. Further, it remotely remediates the vulnerability. When a machine is identified as vulnerable to an attack, an incident, a remediation function is also provided to the administrator to remotely deploy the appropriate update to the machine or device, install it, verifies the files and hashes, and documents it with change tracking and audit trail reports.

[00158] In one embodiment, attacks are accurately identified and mitigated before they reach their targets, and targeted vulnerabilities may be remotely remediated. Therefore, complex threats are more effectively and efficiently mitigated. Correspondingly, the management and maintenance burden on administrators is reduced, saving time and effort.

[00159] Table 9 illustrates some possible features.

Table 9

Supports Windows and UNIX variants

ForcePoint LLC
EX-1009
Page044

Determines in real-time if targeted machine is vulnerable to an attack, virtually eliminating false positives

in-line Sensor flex response terminates the attack

Remotely patches targeted vulnerabilities in one click

Installs in minutes

[00160] FIG. 11 illustrates an intelligent IPS, in accordance with one embodiment.

[00161] As shown in 1101, the on-site server periodically initiates communication with the NOC servers. In 1102, updates are pulled from the NOC servers to the on-site server.

[00162] In 1103a, an IPS in-line sensor monitors and processes network traffic, and sends real time alert data to the on-site server where it cross-references the data with the backend. In 1103b, if the destination IP is vulnerable to the attack, the in-line Sensor is commanded in real-time to drop the malicious packets. As shown in 1104, agents are deployed to each client, accurately identifying which OS, apps, and updates are installed. In 1105, the logic engine automatically determines which updates are needed to remediate the targeted machine, and may be remotely deployed from the IPS console. In 1106, appropriate updates are remotely deployed, installed, and validated on each client.

[00163] In one embodiment, an anti-vulnerability SDK is provided. The SDK was designed to be a simple integration pathway to the Anti-Vulnerability platform backend. The SDK is documented and deliverable. The SDK is compatible with many different programming languages such as C, C++, VB, Java, and others.

[00164] The technology is sophisticated, yet all of the details of managing the communications are implemented in the library, requiring the developer to only learn a simple function calls as detailed hereinafter. A product architect chooses the functionality desired, inserts the provided functionality SDK code into the product code. The SDK code may then query – via the logic engine – the data warehouse, and in turn may return an answer to the point product. The architect can then show the results in any format desired in the product's interface. Full vulnerability remediation and policy compliance and enforcement functionalities may be integrated as well.

ForcePoint LLC
EX-1009
Page045

[00165] FIG. 12 illustrates an SDK function call flow, in accordance with one embodiment.

[00166] Hence, the SDK serves as the architect's tool belt or building blocks needed to quickly and transparently access the Anti-Vulnerability backend and seamlessly integrate the desired functionality into the product without changing or complicating the end user experience.

[00167] Furthermore, the SDK enables system architects to use the Anti-Vulnerability platform to integrate multiple security products and functionalities. Products may then share the same vulnerability data set, improve system automation and accuracy – increasing efficiencies and minimizing false positives and false negatives, and coordinate policy compliance and enforcement functionalities.

[00168] Anti-Vulnerability functions that are accessible via the SDK. The functions are presented in groups, as follows in Table 10.

Table 10

Session Management
Group Management Functions
Client Management Functions
Patch Management Functions
Polling Functions
User Management Functions
Miscellaneous Functions
Policy Compliance Functions
Session Management Functions

[00169] Table 11 sets forth Session Management Functions

Table 11

ForcePoint LLC
EX-1009
Page046

OpenSession – Parameters: HOST name or IP address, LOGIN and PASSWORD for host
Returns: new SESSION Description: This function opens a new session to the OnSite Server
CloseSession – Parameters: SESSION to close
Returns: None Description: Closes a session that is no longer needed
IsSessionGood – Parameters: SESSION to test
Returns: TRUE or FALSE Description: returns TRUE if the session is still valid FALSE if it is not
SUGetLastError – Parameters: None
Returns: Error code of last error in the thread Description: Returns the error code of the last SDK error to occur in this thread
SUSetLastError – Parameters: ERROR code to set
Returns: None Description: Sets the error code for the thread to be returned by SUGetLastError
GetSDKVersion – Parameters: None
Returns: a WORD containing the version of the SDK Description: the MSB of the returned value is the major version number, the LSB is the minor version number
Ping – Parameters: SESSION to use, VALUE to ping with
Returns: VALUE on success 0 on failure Description: attempts to pass VALUE to the OnSite Server, which should pass it back.

[00170] Table 12 sets forth Group Management Functions.

Table 12

CreateGroup – Parameters: Group NAME and Description
Returns: GROUP that was just created or 0 on failure

ForcePoint LLC
EX-1009
Page047

Description: This function creates a new group with the provided name and Description
GetGroups – Parameters: None
Returns: A LIST of GROUPs. Description: This function Returns a list of all configured groups.
GetGroupsEx – Parameters: None
Returns: A LIST of GROUPINFO structures Description: This function Returns a list of all configured groups' information
DeleteGroup – Parameters: GROUP to be deleted.
Returns: Success or failure Description: This function permanently removes a group.
EditGroup – Parameters: GROUP to be edited, GROUPINFO to be applied
Returns: Success or failure Description: This function changes a GROUP's information
GetGroupPolicyOSCategories – Parameters: GROUP to get information about
Returns: A LIST of OPERATINGSYSYTEMCATEGORYs that have group policies configured Description: This function retrieves a list of operating system categories that have group policies configured
GetGroupPolicyOSSubCategories – Parameters: GROUP to get information about, OPERATINGSYSTEMCATEGORY to get sub category information about
Returns: A LIST of OPERATINGSYSTEMSUBCATEGORYs Description: This function retrieves a list of operating system sub-categories of OPERATINGSYSTEMCATEGORY that have policies for the GROUP
GetGroupPolicyInfo – Parameters: GROUPPOLICY to get information about, GROUPPOLICYINFO pointer to receive the information
Returns: Success or Failure Description: This function fills the passed GROUPPOLICYINFO structure with the information for the GROUPPOLICY
GetGroupPolicyInfoByOSCat – Parameters: GROUP to get information about, OPERATINGSYSTEMCATEGORY to get the policy for, GROUPPOLICYINFO

ForcePoint LLC
EX-1009
Page048

pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for a policy for the OPERATINGSYSTEMCATEGORY in the GROUP
GetGroupPolicyInfoByOSSubCat – Parameters: GROUP to get information about, OPERATINGSYSTEMSUBCATEGORY to get the policy for, GROUPPOLICYINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for a policy for the OPERATINGSYSTEMSUBCATEGORY in the GROUP
DeleteGroupPolicy – Parameters: GROUPPOLICY to delete
Returns: Success or failure Description: This function permanently deletes the GROUPPOLICY
EditGroupPolicy – Parameters: GROUPPOLICYINFO with new information
Returns: Success or failure Description: This function updates the group policy (contained in GROUPPOLICYINFO) with the information in GROUPPOLICYINFO
AddGroupPolicy – Parameters: GROUP to add the policy to, GROUPPOLICYINFO containg the policy information
Returns: Success or Failure Description: This function creates a new group policy and applies it to the GROUP
GetClientsInGroup – Parameters: GROUP to retrieve the clients from
Returns: LIST of CLIENTs belonging to the group Description: This function retrieves a list of clients that are members of a specific group
GetClientsInGroupEx – Parameters: GROUP to retrieve the clients from
Returns: LIST of CLIENTINFOs for clients belonging to the group Description: This function Returns a list of CLIENTINFO structures containing information for the clients that belong to this group
AddClientToGroup – Parameters: CLIENT to add to a group, GROUP to add the client to.

ForcePoint LLC
EX-1009
Page049

Returns: Success or failure Description: This function adds a client to a group
RemoveClientFromGroup – Parameters: CLIENT to remove from group, GROUP to remove the client from
Returns: Success or failure. Description: This function removes a client from a group.
MoveClientToGroup – Parameters: CLIENT to move, GROUP to move client to
Returns: Success or Failure Description: This function moves CLIENT to GROUP
GetUngroupedClients -- Parameters: None
Returns: LIST of ungrouped clients Description: This function Returns a LIST of the clients that do not belong to any group
GetUngroupedClientsEx – Parameters: None
Returns: LIST of CLIENTINFO structures Description: This function Returns a LIST of CLIENTINFO structures for the clients that do not belong to any group
GetGroupInfo – Parameters: GROUP to get information about, GROUPINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for the GROUP

[00171] Table 13 sets forth Client Management Functions.

Table 13

GetClientInstalledSoftware – Parameters: CLIENT to get information about
Returns: LIST of SOFTWARE installed on the client Description: This function retrieves a list of the software that has been detected on the

ForcePoint LLC
EX-1009
Page050

client
GetClientInstalledSoftwareEx – Parameters: CLIENT to get information about
Returns: LIST of SOFTWAREINFO for software installed on the client Description: This function returns a LIST of SOFTWAREINFO structures describing the software detected on the client
GetClientInstalledPatches – Parameters: CLIENT to get information from.
Returns: LIST of PATCHes corresponding to the installed patches on the client Description: This function retrieves a list of patches that were verified as installed on the last polling
GetClientInstalledPatchesEx – Parameters: CLIENT to get information from
Returns: LIST of PATCHINFO structures corresponding to the installed patches on the client Description: This function retrieves a LIST of PATCHINFO structures for patches that were verified as installed on the last polling
GetClientPendingPatches – Parameters: CLIENT to get information from.
Returns: LIST of PATCHes corresponding to the pending patches for the client Description: This function returns a list of patches that the client needs (according to group policy) as of the last polling.
GetClientPendingPatchesEx – Parameters: CLIENT to get information from
Returns: A LIST of PATCHINFO structures corresponding to the pending patches for the client Description: This function returns a LIST of PATCHINFO structures for patches that the client needs (according to group policy) as of the last polling.
GetClientPendingServicePack – Parameters: CLIENT to get information from
Returns: SERVICEPACK if a service pack is pending or 0 if not Description: This function returns a SERVICEPACK if there is a service pack pending for the client (according to group policy) as of the last polling. If there is no service pack pending it returns 0
GetClientPendingSoftware – Parameters: CLIENT to get information from
Returns: LIST of SOFTWARE that is pending

ForcePoint LLC
EX-1009
Page051

Description: This function returns a list of software that is pending for the client (according to group policy) as of the last polling
GetClientLogs - Parameters: CLIENT to get information from
Returns: LIST of LOGs for the client. Description: This function returns a list of logs for a particular client.
GetClientLogsEx – Parameters: CLIENT to get information from
Returns: LIST of LOGINFO structures Description: This function returns a list of LOGINFO structures containing log entries for a particular client.
DeleteClient – Parameters: CLIENT to delete.
Returns: Success or failure. Description: This function removes all information pertaining to this client from the SysUpdate database.
GetClientOS – Parameters: CLIENT to get information from
Returns: OPERATINGSYSTEM installed on client Description: This function returns the OPERATINGSYSTEM installed on the client
GetClientServicePack – Parameters: CLIENT to get information from
Returns: SERVICEPACK installed on client or 0 Description: This function returns the service pack installed on the client or 0 if the client does not have a service pack installed, or if service packs are not applicable to the client's platform
GetClientInfo – Parameters: CLIENT to get information from CLIENTINFO pointer to receive the information
Returns: Success or failure Description: This function fills the passed CLIENTINFO structure with information pertaining to the passed CLIENT
GetClientFromIP – Parameters: IP address of client
Returns: CLIENT that corresponds to the passed IP address Description: This function maps IP addresses to clients

ForcePoint LLC
EX-1009
Page052

[00172] Table 14 sets forth Patch Management Functions.

Table 14

GetPatchInfo – Parameters: PATCH to get information about, PATCHINFO pointer to receive information
Returns: Success or failure Description: This function fills the passed patch info structure with information about the passed patch
InstallPatchForClient – Parameters: CLIENT to install the patch on, PATCH to install
Returns: Success or failure Description: This function deploys the patch to the client. Installation proceeds asynchronously
InstallPatchForGroup – Parameters: GROUP to install the patch on, PATCH to install
Returns: Success or failure Description: This function deploys the patch to all clients in the group
InstallAllPendingForClient – Parameters: CLIENT to install patches on
Returns: Success or failure Description: This function deploys all pending patches for a client to the client
InstallAllPendingForGroup – Parameters: GROUP to install patches on
Returns: Success or failure Description: This function deploys all pending patches to all clients in a group
RejectPatchForClient – Parameters: CLIENT to reject patch for, PATCH to reject
Returns: Success or failure Description: This function rejects a patch for a client. This patch will not be queued down or installed
RejectPatchForGroup – Parameters: GROUP to reject patch for, PATCH to reject
Returns: Success or failure Description: This function rejects a patch for every client in a group. This patch will not be queued down or installed
RequeuePatchForClient – Parameters: CLIENT to requeue the patch for, PATCH to requeue

ForcePoint LLC
EX-1009
Page053

Returns: Success or failure Description: This function requeues a previously rejected patch for a client
RequeuePatchForGroup – Parameters: GROUP to requeue the patch for, PATCH to requeue
Returns: Success or failure Description: This function requeues a previously rejected patch for every client in a group
RemovePatchFromClient – Parameters: CLIENT to remove patch from, PATCH to remove
Returns: Success or failure Description: This function will uninstall a patch from a client
RemovePatchFromGroup – Parameters: GROUP to remove patch from, PATCH to remove
Returns: Success or failure Description: This function will uninstall a patch for every client in a group
InstallServicePackForClient – Parameters: CLIENT to install service pack on, SERVICEPACK to install on client
Returns: Success or failure Description: This function will install a service pack on a client
InstallServicePackForGroup – Parameters: GROUP to install service pack on, SERVICEPACK to install
Returns: Success or failure Description: This function will install a service pack on every client in a group
InstallSoftwareForClient – Parameters: CLIENT to install software update on, SOFTWARE to install
Returns: Success or failure Description: This function will install a software update on a client
InstallSoftwareForGroup – Parameters: GROUP to install software update on, SOFTWARE to install
Returns: Success or failure Description: This function will install a software update on every client in a group.
GetCveIDsFromPatch – Parameters: PATCH to get CveIDs from
Returns: A LIST of CVEIDs

ForcePoint LLC
EX-1009
Page054

Description: This function returns a list of CVEIDs the correspond to the PATCH

[00173] Table 15 sets forth Polling Functions.

Table 15

PollClient – Parameters: CLIENT to poll
Returns: Success or failure. Description: This function causes a client to be polled by the OnSite Server immediately.
PollGroup – Parameters: GROUP to poll
Returns: Success or failure. Description: This function causes all the clients in a particular group to be polled immediately.
PollAll – Parameters: NONE
Returns: Success or failure. Description: This function causes all clients to be polled immediately.

[00174] Table 16 sets forth User Management Functions.

Table 16

GetUsers – Parameters: None
Returns: A LIST of USERs Description: This function returns a list of all users for the system
GetUserInfo – Parameters: USER to get information about, USERINFO pointer to receive the information
Returns: Success or failure Description: This function populates the passed USERINFO structure with information

ForcePoint LLC
EX-1009
Page055

about the passed USER
GetUserGroupPrivileges – Parameters: USER to get information about
Returns: A LIST of USERGROUPPRIVILEGEs Description: This function returns a LIST of USERGROUPPRIVILEGES representing the privileges that a particular user has
GetUserGroupPrivilegesEx – Parameters: USER to get information about
Returns: A LIST of USERGROUPPRIVILEGEINFO structures Description: This function returns a LIST of USERGROUPPRIVILEGEINFO structures representing the privileges that a particular user has
GetUserGroupPrivilegeInfo – Parameters: USERGROUPPRIVILEGE to get information about, USERGROUPPRIVILEGEINFO pointer to receive information
Returns: Success or failure Description: This function populates the passed USERGROUPPRIVILEGEINFO structure with the details of the particular privilege
GetUserGroupPrivilegeInfoByGroup – Parameters: USER to get information about, GROUP to get information for, USERGROUPPRIVILEGEINFO pointer to populate
Returns: Success or Failure Description: This function populates the passed USERGROUPPRIVILEGEINFO structure with the detailed information regarding the permissions that the passed user has on the passed group
AddUserGroupPrivilege – Parameters: USERGROUPPRIVILEGEINFO structure to add
Returns: Success or failure Description: This function adds a USERGROUPPRIVILEGE
EditUserGroupPrivilege – Parameters: USERGROUPPRIVILEGEINFO with new values
Returns: Success or failure Description: This function edits the USERGROUPPRIVILEGEINFO structure passed in, assign it the new values
DeleteUserGroupPrivilege – Parameters: USERGROUPPRIVILEGE to delete
Returns: Success or failure Description: This function deletes the passed USERGROUPPRIVILEGE from the

ForcePoint LLC
EX-1009
Page056

system
AddUser – Parameters: USERNAME, PASSWORD, and USERTYPE
Returns: USER representing the user that was just created Description: This function creates a new user with the provided username, password, and type, and returns a USER representing the new user or 0 in the case of an error
DeleteUser – Parameters: USER to delete
Returns: Success or failure Description: This function permanently deletes the USER from the system along with any privileges the user may have had
ChangeUserPassword – Parameters: USER to change password for, new PASSWORD
Returns: Success or failure Description: This function changes the password for a user
ChangeUserRole – Parameters: USER to change role, ROLE to change to
Returns: Success or failure Description: This Function changes a user's role
GetUserFromName – Parameters: USERNAME
Returns: USER corresponding to the passed user name Description: This function provides a mapping from user names to USERs

[00175] Table 17 sets forth Miscellaneous Functions.

Table 17

CreateList – Parameters: None
Returns: A new, empty, LIST Description: This functions creates a new LIST that is initially empty
GetListItemEx – Parameters: LIST to retrieve item from, INDEX of item to retrieve, VOID pointer to receive item
Returns: Success or failure

ForcePoint LLC
EX-1009
Page057

Description: This function populates the memory pointed to by VOID with the contents of the LIST item at INDEX
GetListSize – Parameters: LIST to get the size of
Returns: the size of the LIST Description: This function returns the number of elements currently in the list
AddItemToList – pointer to LIST to add the item to, LONG item to add
Returns: None Description: This function adds an "item" (such as a GROUP or a CLIENT) to a LIST
AddClientInfoExToList – See AddItemToList
AddGroupInfoToList – See AddItemToList
AddPatchInfoExToList – See AddItemToList
AddSoftwareInfoToList – See AddItemToList
AddSoftwareCategoryInfoToList – See AddItemToList
AddUserGroupPrivilegeInfoExToList – See AddItemToList
RemoveItemFromList – Parameters: pointer to LIST to remove the item from, INDEX of item to remove
Returns: None Description: This function removes the item at INDEX from the LIST
FreeList – LIST to deallocate
Returns: None Description: This function deallocates the resources used by LIST
GetSoftwareInfo – Parameters: SOFTWARE to get information for, SOFTWAREINFO pointer to hold the information
Returns: Success or failure Description: This function populates the SOFTWAREINFO structure pointed at with information regarding the SOFTWARE
GetLogInfo – Parameters: LOG to get information about, LOGINFO pointer to contain the information
Returns: Success or failure Description: This function populates the LOGINFO structure pointed at with

information regarding the LOG
GetSoftwareCategories – Parameters: None
Returns: A LIST of SOFTWARECATEGORYs Description: This function returns a LIST of SOFTWARECATEGORYs
GetSoftwareCategoriesEx – Parameters: None
Returns: A LIST of SOFTWARECATEGORYINFO structures Description: This function returns LIST of SOFTWARECATEGORYINFO structures for every software category known on the system
GetSoftwareCategoriesForOperatingSystemCategory – Parameters: an OPERATINGSYSTEMCATEGORY to get information for
Returns: A LIST of SOFTWARECATEGORYs Description: This function returns a LIST of software categories for the passed operating system category.
GetSoftwareCategoriesForOperatingSystemCategoryEx – As above only, returning the appropriate "info" structures in the list
GetSoftwareCategoryInfo – Parameters: SOFTWARECATEGORY to get information for, SOFTWARECATEGORYIFNO pointer to contain the information Returns: Success or failure

[00176] Table 18 sets forth Policy Compliance Functions.

[00177] These functions are provided in a separate source tree (policy tree) for the Policy Compliance and Enforcement module. Function include: Password/system access policies, log configurations, audit settings, user/group privilege rights, general service settings, service permissions, registry values, registry permissions, file permissions. It can also perform deltas on and get information about: groups, users, services, and all the "Run" registry keys.

[00178] The function calls are being integrated into the live production tree and subject to change.

Table 18

GetPolicyItemInfo – As GetOperatingSystemInfo for POLICYITEM and POLICYITEMINFO

ForcePoint LLC
EX-1009
Page059

InstallPolicyItemForClient – As InstallPatchForClient for POLICYITEM
InstallPolicyItemForGroup – As InstallPatchForGroup for POLICYITEM
InstallAllPendingPolicyItemsForClient – As InstallAllPendingPatchesForClient for POLICYITEM
InstallAllPendingPolicyItemsForGroup – As InstallAllPendingPatchesForGroup for POLICYITEM
RemovePolicyItemFromClient – As RemovePatchForClient for POLICYITEM
RemovePolicyItemFromGroup – As RemovePatchFromGroup for POLICYITEM

[00179] All publications, prior applications, and other documents cited herein are hereby incorporated by reference in their entirety as if each had been individually incorporated by reference and fully set forth.

[00180] While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is to be considered as illustrative and not restrictive in character, it being understood that only the preferred embodiments have been shown and described and that all changes and modifications that would occur to one skilled in the relevant art are desired to be protected.

ForcePoint LLC
EX-1009
Page060

CLAIMS

What is claimed is:

1. A computer program product embodied on a non-transitory computer readable medium for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation technique, the computer program product comprising:

code for:

accessing at least one data storage identifying a plurality of mitigation techniques that mitigate effects of attacks that takes advantage of the vulnerabilities, such that:

each mitigation technique capable of mitigates an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

receiving information from at least one of a plurality of devices;

identifying an attack on the at least one device based on the information that takes advantage of at least one of the vulnerabilities; and

sending a signal to the at least one device;

code for:

receiving the signal; and

applying at least two of the plurality of mitigation techniques to the at least one device, in response to the signal.

2. The computer program product of Claim 1, wherein the computer program product is operable for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

ForcePoint LLC
EX-1009
Page061

ABSTRACT

A system, method, and computer program product are provided for a database associating a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities. Each of the device vulnerabilities is associated with at least one remediation technique. Each remediation technique associated with a particular device vulnerability remediates that particular vulnerability. Further, each remediation technique has a remediation type are selected from the type group consisting of patch, policy setting, and configuration option. Still yet, a first one of the device vulnerabilities is associated with at least two alternative remediation techniques.

ForcePoint LLC
EX-1009
Page062

COMBINED DECLARATION (37 C.F.R. 1.63) AND ASSIGNMENT FOR UTILITY APPLICATION USING AN APPLICATION DATA SHEET (37 C.F.R. 1.76)

Title of Invention: **COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION**

As the below named inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked)
☐ United States application or PCT international application number _____, filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, CFR § 1.56.

Whereas, I the undersigned inventor have invented certain new and useful improvements as set forth in the above-identified patent application and further identified by the Attorney Docket Number provided above in the header of this document.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I the undersigned inventor hereby:

1) Sell(s), assign(s) and transfer(s) to SecurityProfiling, LLC, a Texas limited liability company having a place of business at 1919 S Shiloh Rd. Garland, TX 75042, (hereinafter referred to as ("ASSIGNEE"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application.

2) Authorize and request the Commissioner of Patents to issue any and all Letters Patents resulting from said application or any division(s), continuation(s), substitutes(s) or reissue(s) thereof to the ASSIGNEE.

3) Agree to execute all papers and documents and, entirely at the ASSIGNEE's expense, perform any acts which are reasonably necessary in connection with the prosecution of said application, as well as any derivative and applications thereof, foreign applications based thereon, and/or the enforcement of patents resulting from such applications.

4) Agree that the terms, covenants and conditions of this assignment shall inure to the benefit of the Assignee, its successors, assigns and other legal representative, and shall be binding upon the inventor(s), as well as the inventor's heirs, legal representatives and assigns.

5) Warrant and represent that I have not entered, and will not enter into any assignment, contract, or understanding that conflicts with this assignment.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Signed on the date indicated beside my signature.

Legal Name of Inventor: John P. Blignaut

Signature: _____ Date: 9.24.14

ForcePoint LLC
EX-1009
Page063

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Brett M. Oliphant Date (Optional) : _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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 1.11 and 1.14. This collection is estimated to take 1 minute 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.

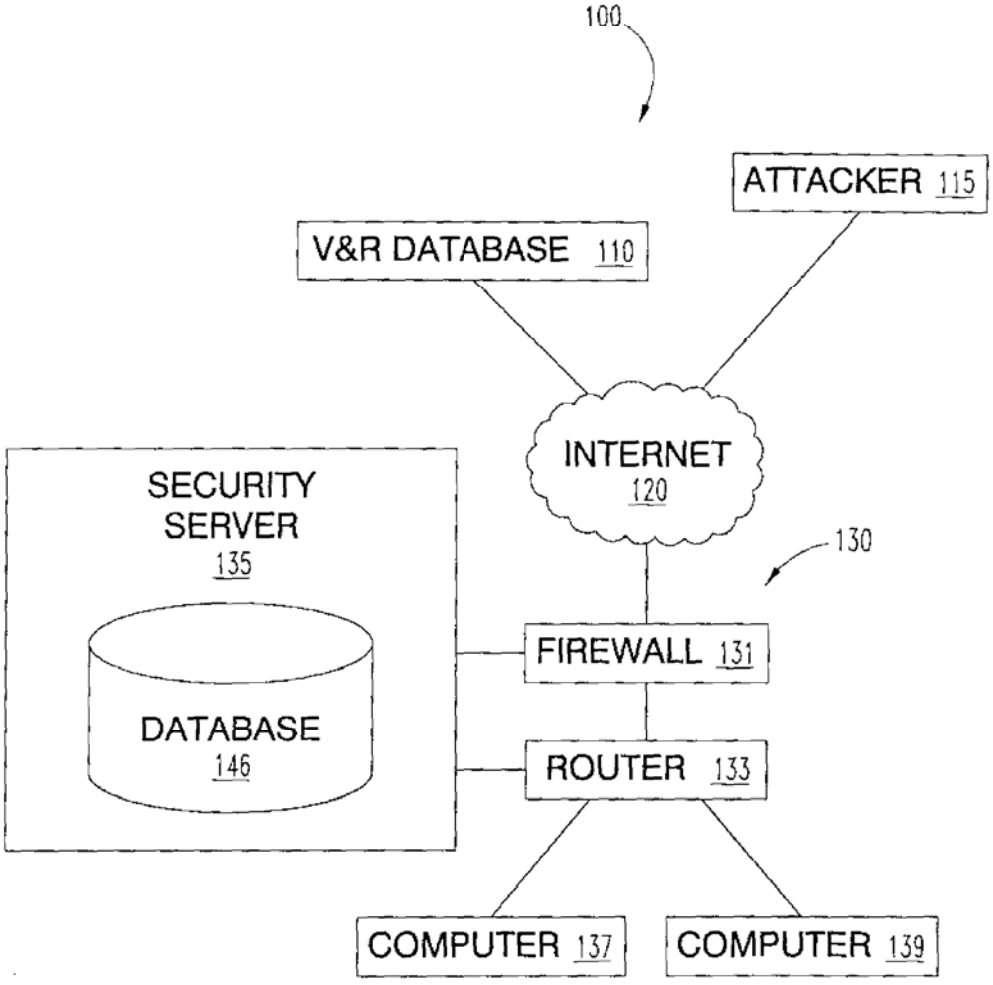

100
ATTACKER 115
V&R DATABASE 110
INTERNET 120
SECURITY SERVER 135
DATABASE 146
130
FIREWALL 131
ROUTER 133
COMPUTER 137
COMPUTER 139

Fig. 1

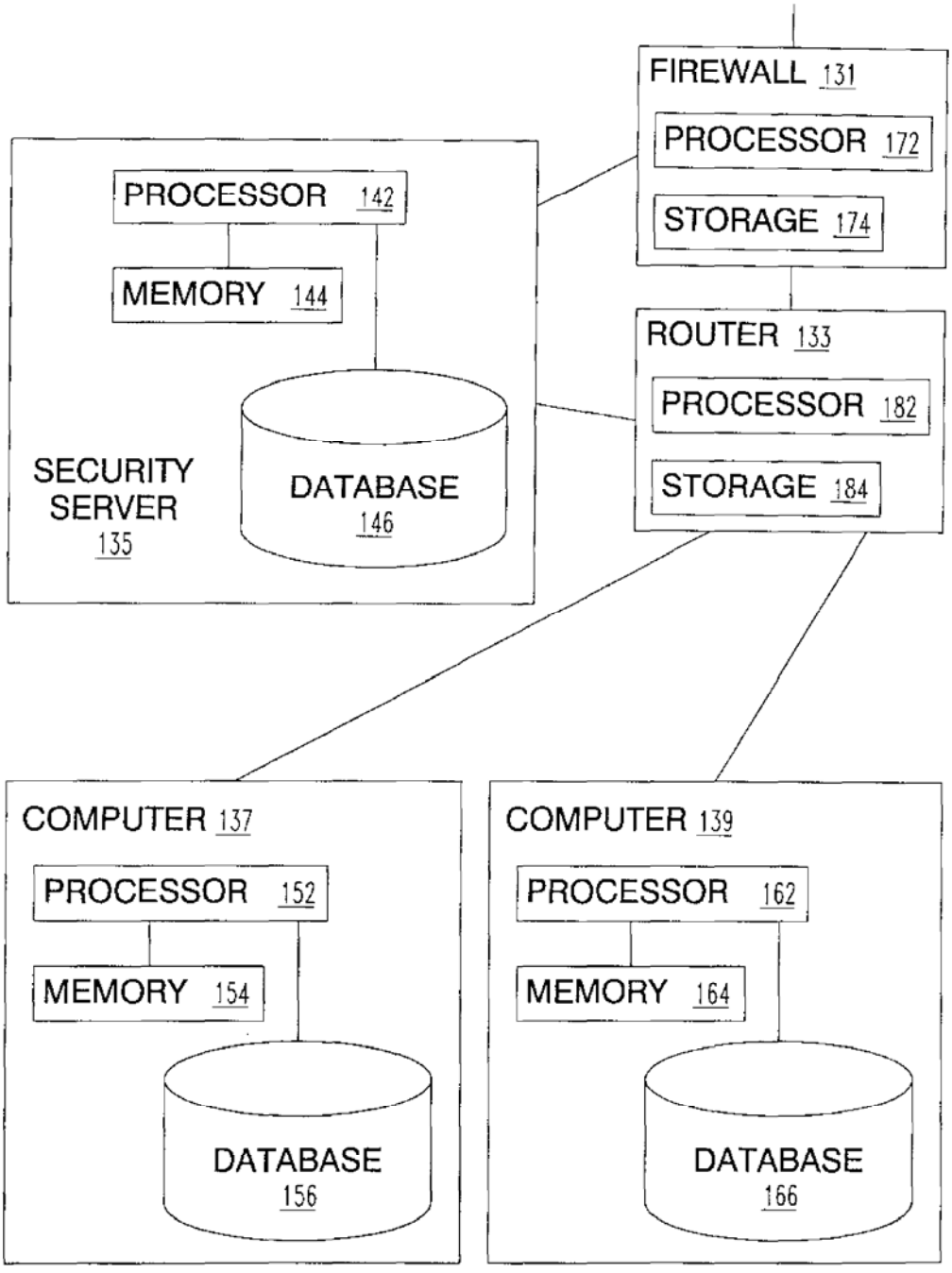

FIREWALL 131
PROCESSOR 172
STORAGE 174
PROCESSOR 142
MEMORY 144
ROUTER 133
PROCESSOR 182
STORAGE 184
SECURITY SERVER 135
DATABASE 146
COMPUTER 137
PROCESSOR 152
MEMORY 154
DATABASE 156
COMPUTER 139
PROCESSOR 162
MEMORY 164
DATABASE 166

Fig. 2

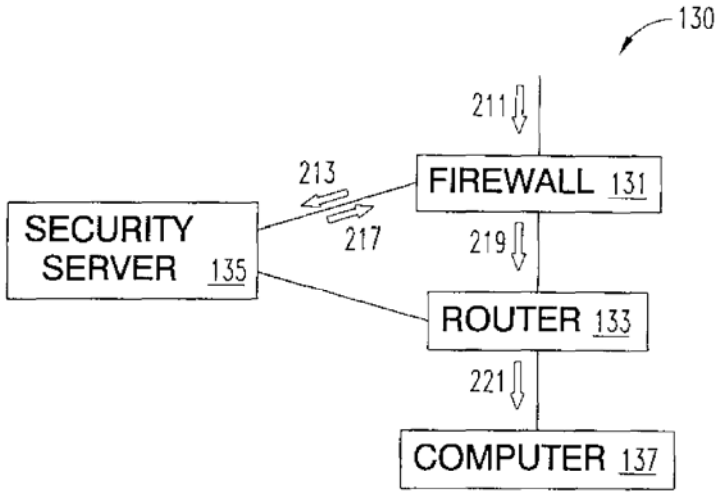

130
211
213
FIREWALL 131
SECURITY SERVER 135
217
219
ROUTER 133
221
COMPUTER 137

Fig. 3

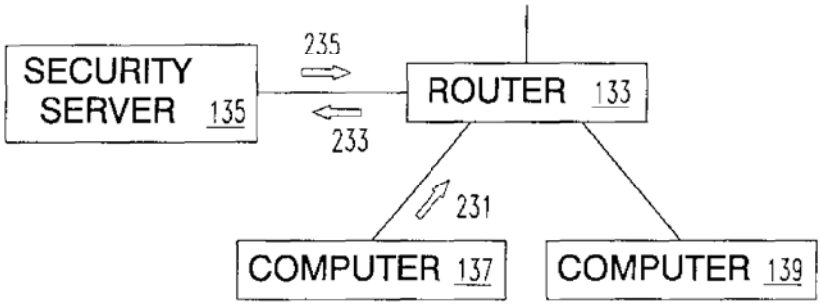

235
SECURITY SERVER 135
ROUTER 133
233
231
COMPUTER 137
COMPUTER 139

Fig. 4

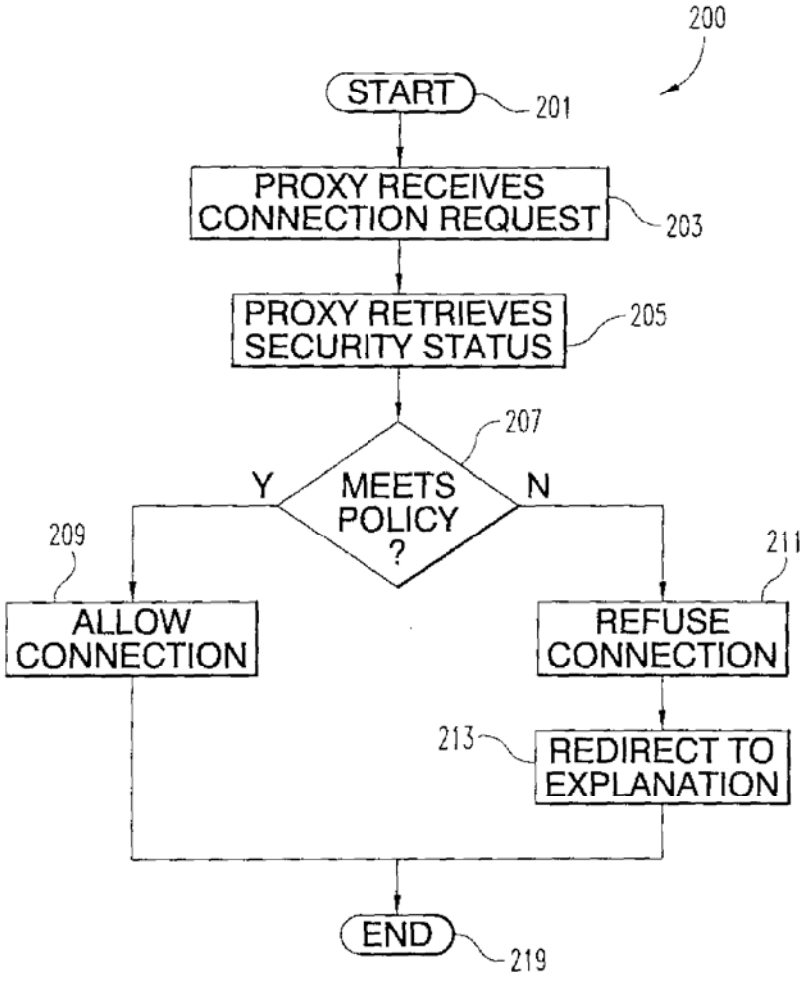

200
START
201
PROXY RECEIVES CONNECTION REQUEST
203
PROXY RETRIEVES SECURITY STATUS
205
207
MEETS POLICY ?
Y
N
209
ALLOW CONNECTION
211
REFUSE CONNECTION
213
REDIRECT TO EXPLANATION
END
219

Fig. 5

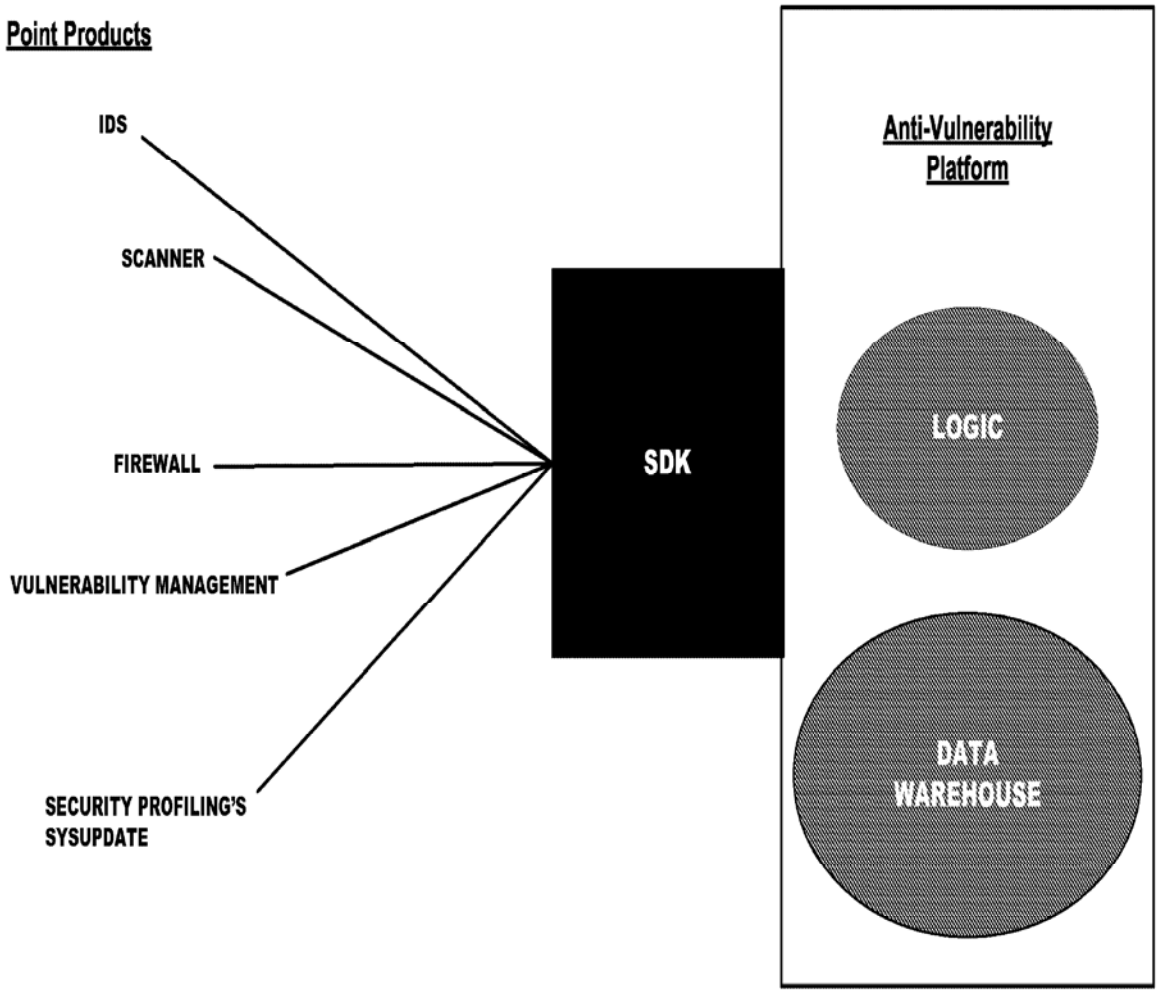

Point Products
IDS
SCANNER
FIREWALL
VULNERABILITY MANAGEMENT
SECURITY PROFILING'S
SYSUPDATE
SDK
Anti-Vulnerability
Platform
LOGIC
DATA
WAREHOUSE

FIG. 5B

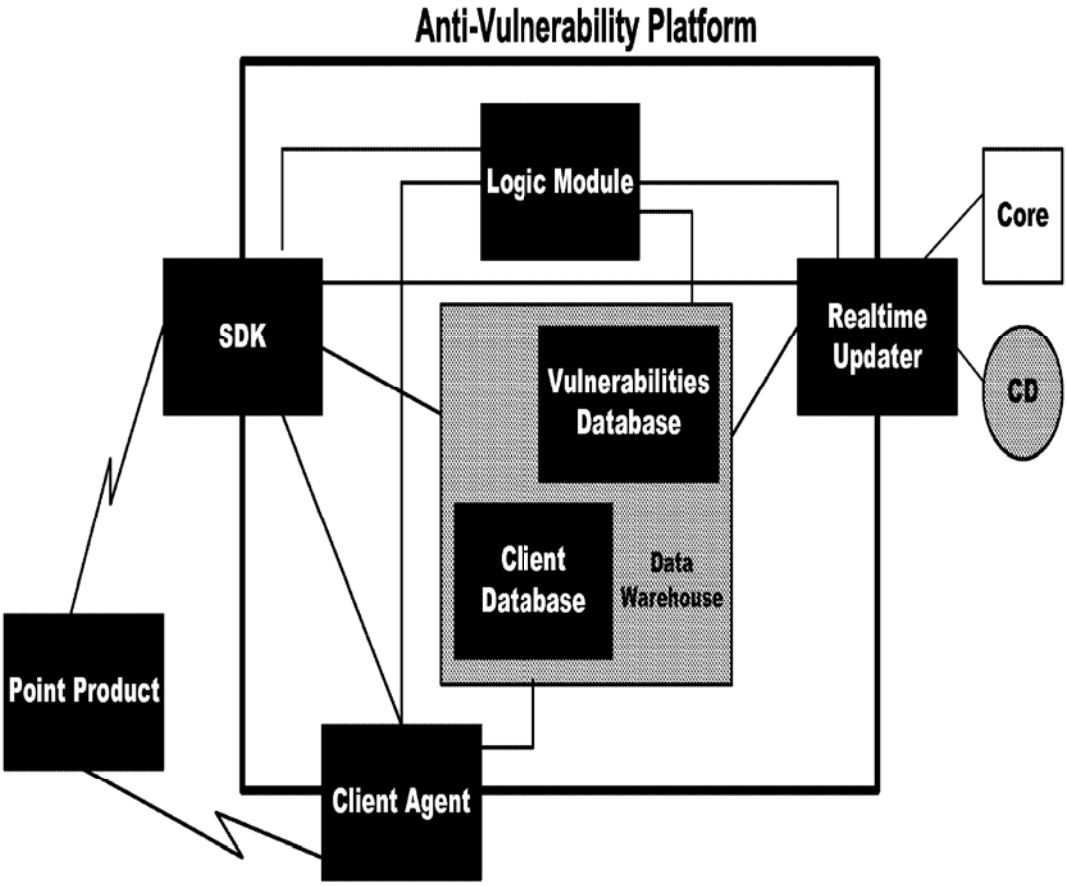

Anti-Vulnerability Platform
Logic Module
Core
SDK
Realtime Updater
Vulnerabilities Database
CD
Client Database
Data Warehouse
Point Product
Client Agent
Anti-Vulnerability Engine
SDK
Logic Module
Anti-Vulnerability Service
Vulnerabilities Database
Realtime Updater
Core
CD

FIG. 6

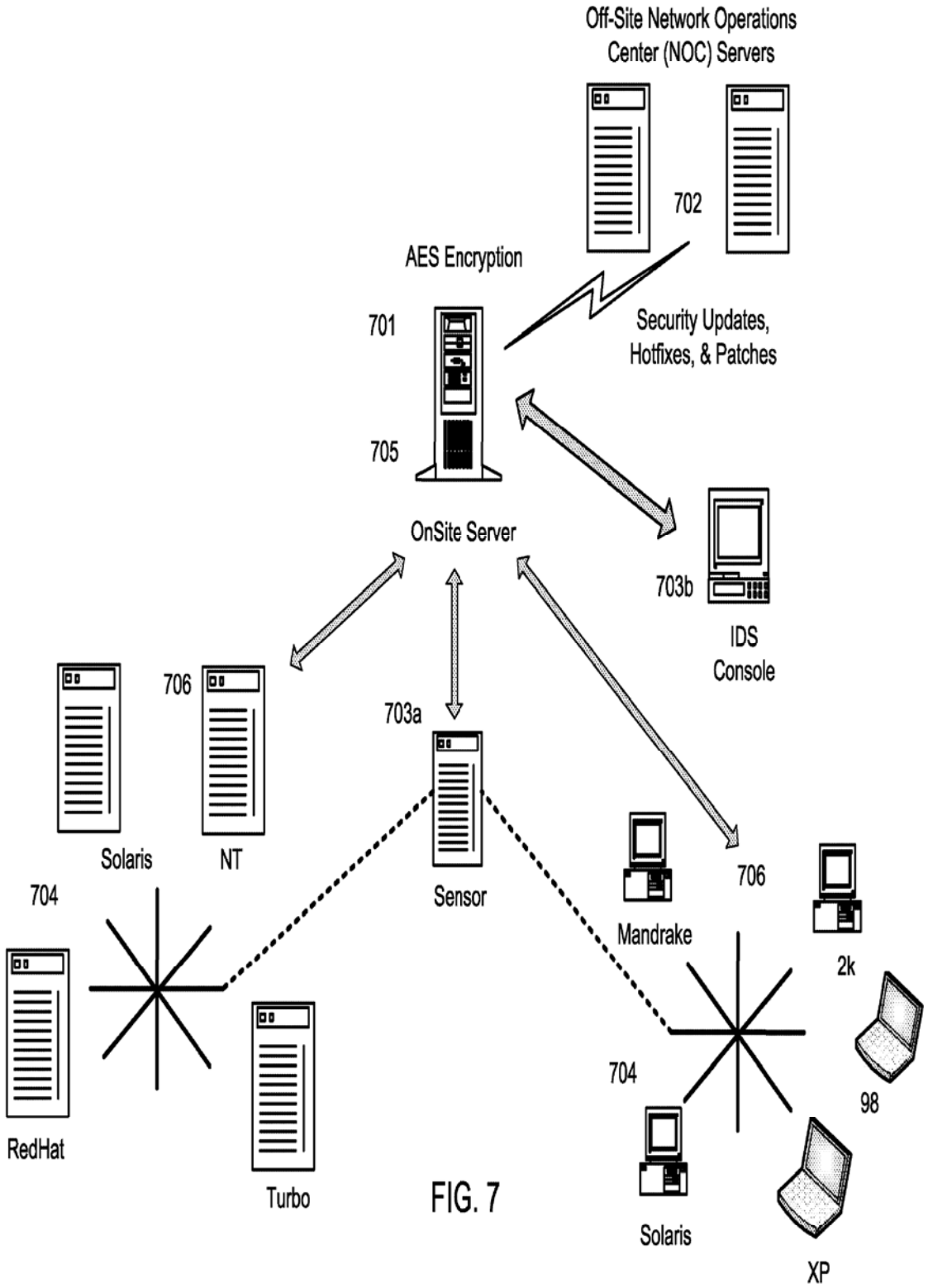

Off-Site Network Operations Center (NOC) Servers
702
AES Encryption
701
Security Updates, Hotfixes, & Patches
705
OnSite Server
703b
IDS Console
706
703a
Solaris
NT
Sensor
704
Mandrake
706
2k
98
RedHat
Turbo
704
Solaris
XP

FIG. 7

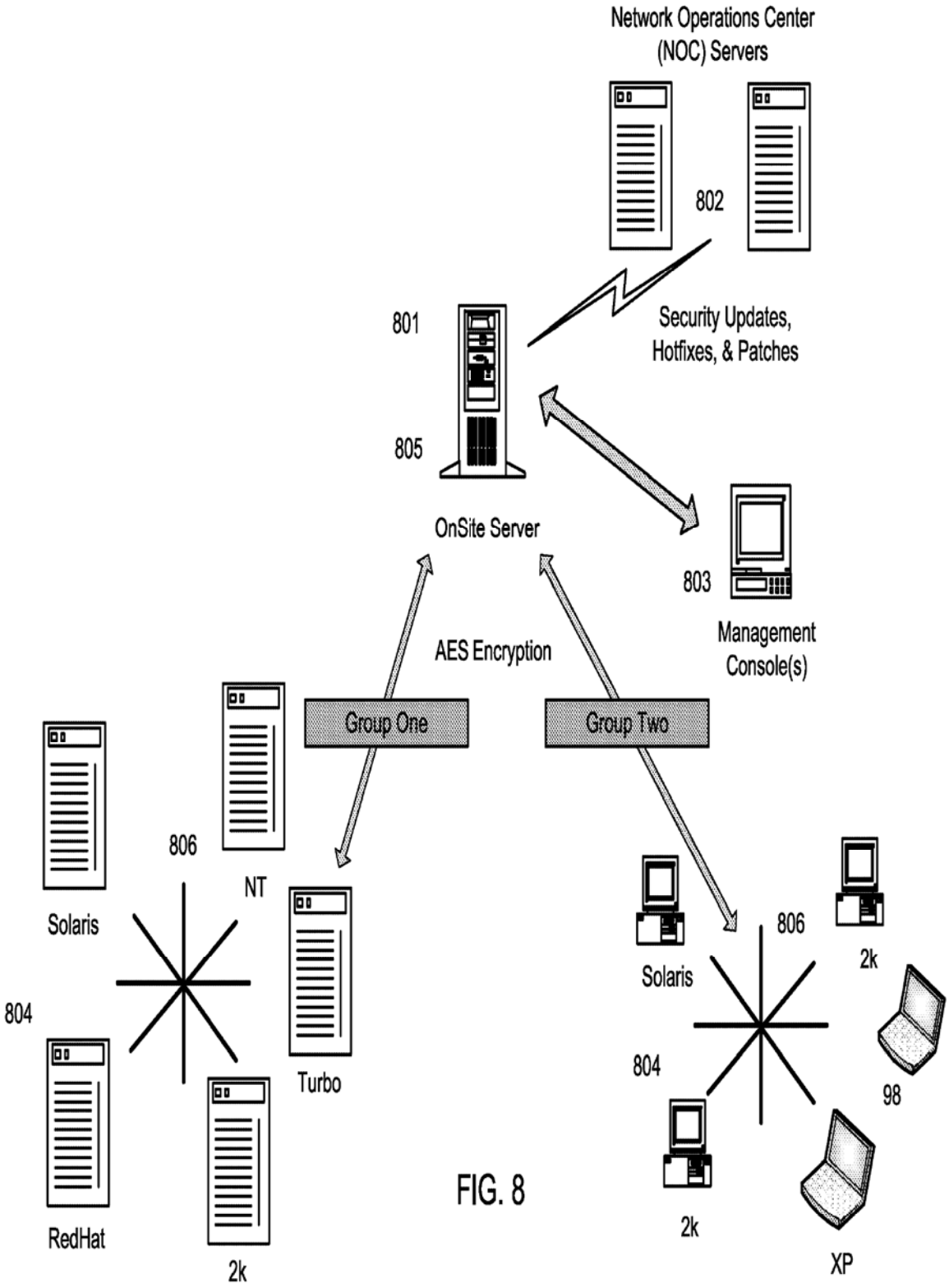

Network Operations Center
(NOC) Servers
802
801
Security Updates,
Hotfixes, & Patches
805
OnSite Server
803
Management
Console(s)
AES Encryption
Group One
Group Two
806
Solaris
NT
804
Turbo
RedHat
2k
Solaris
806
2k
804
98
2k
XP

FIG. 8

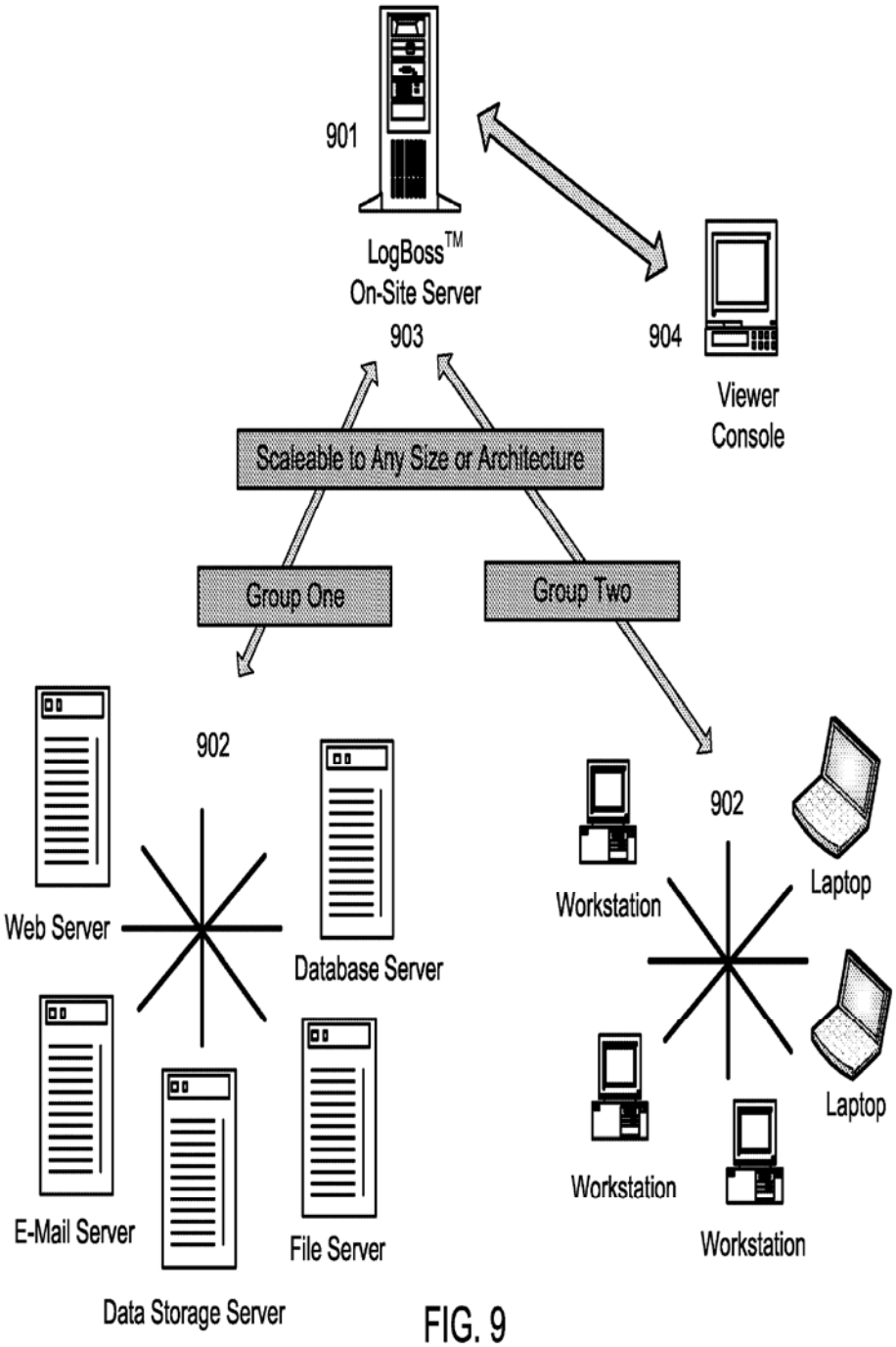

901
LogBoss™
On-Site Server
903
904
Viewer
Console
Scaleable to Any Size or Architecture
Group One
Group Two
902
Web Server
Database Server
E-Mail Server
File Server
Data Storage Server
902
Workstation
Laptop
Laptop
Workstation
Workstation

FIG. 9

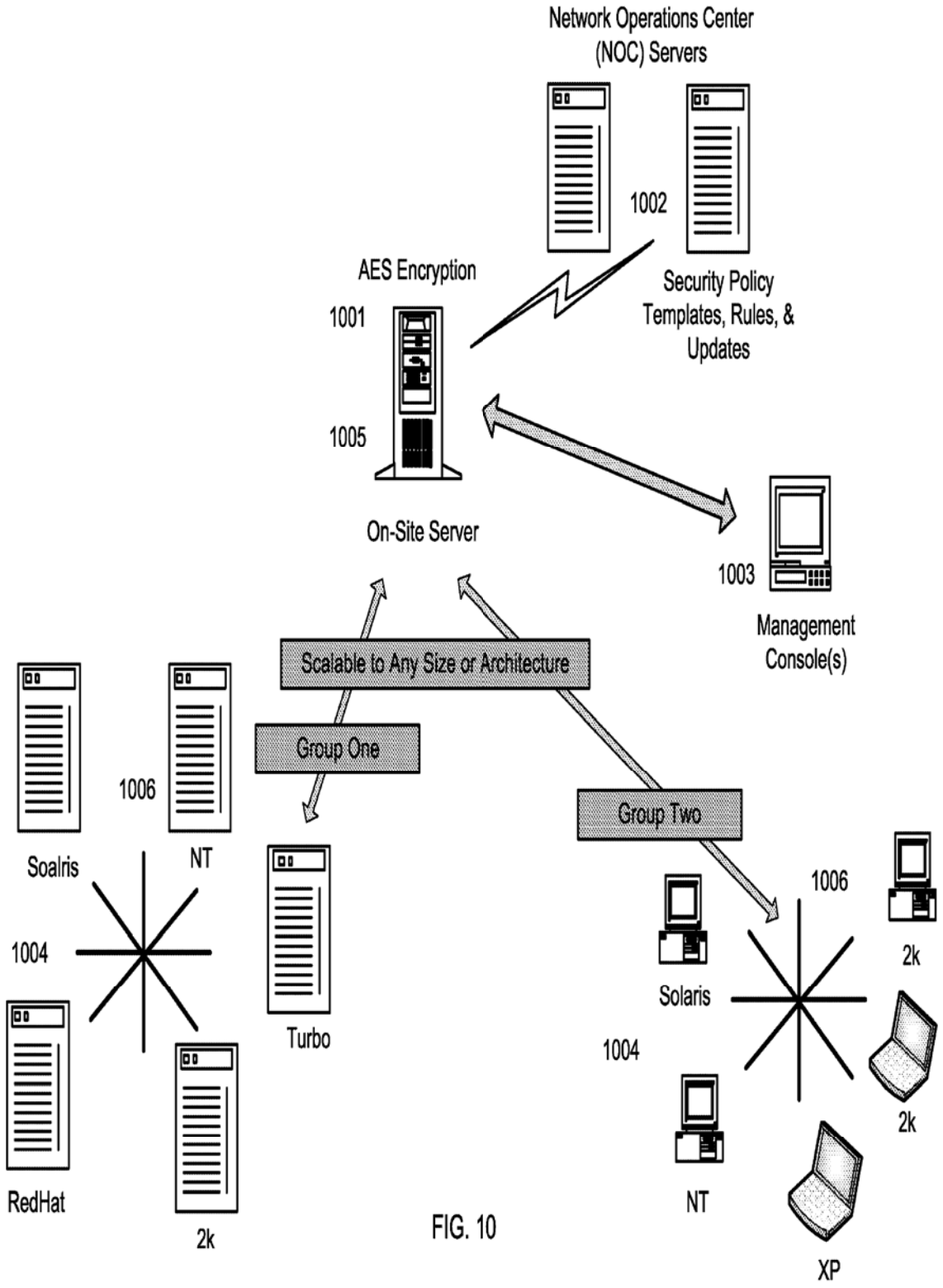

Network Operations Center
(NOC) Servers
1002
AES Encryption
1001
Security Policy
Templates, Rules, &
Updates
1005
On-Site Server
1003
Management
Console(s)
Scalable to Any Size or Architecture
Group One
Group Two
1006
Soalris
NT
1004
RedHat
2k
Turbo
1006
Solaris
2k
1004
2k
NT
XP

FIG. 10

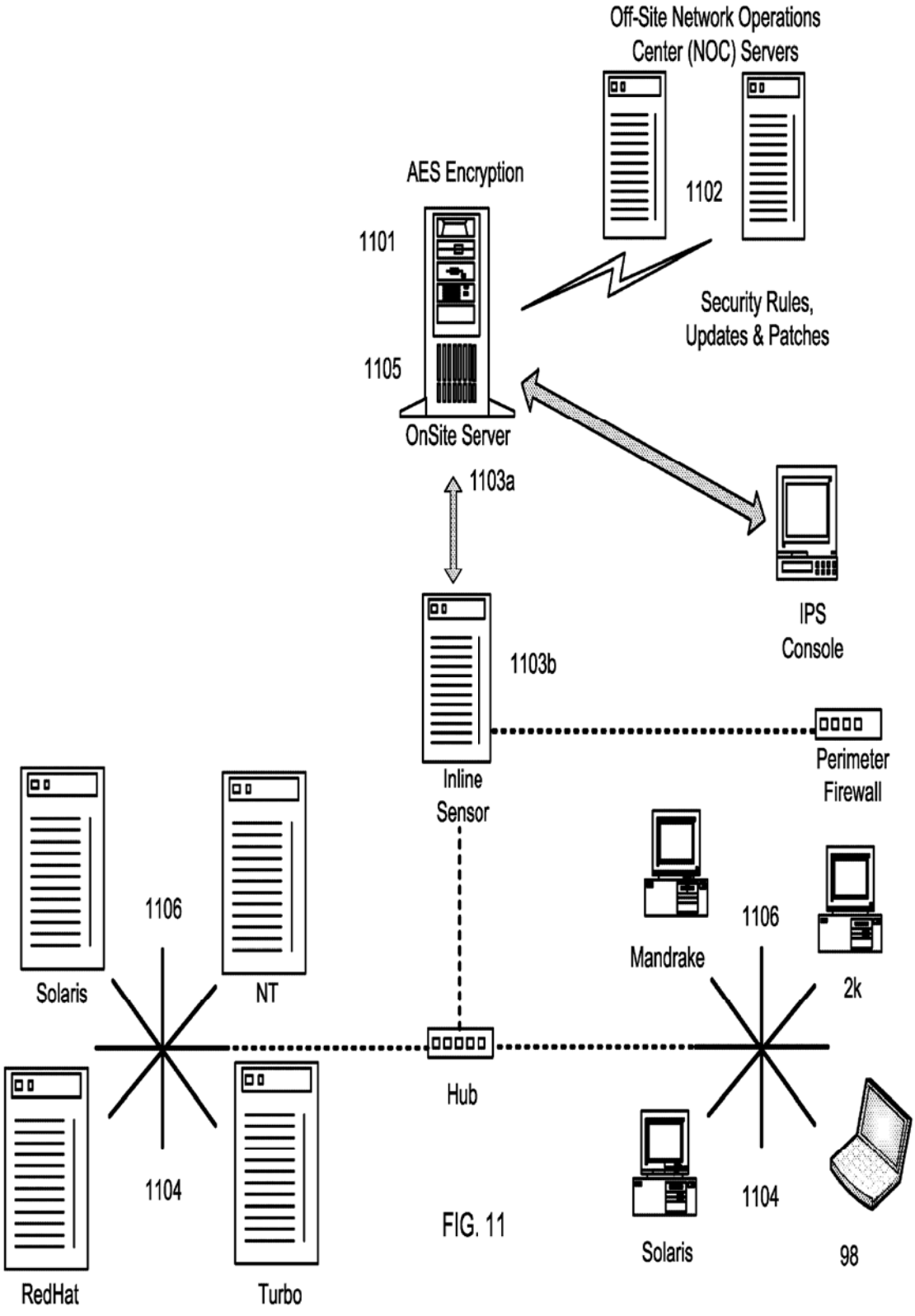

Off-Site Network Operations
Center (NOC) Servers
1102
AES Encryption
1101
Security Rules,
Updates & Patches
1105
OnSite Server
1103a
IPS
Console
1103b
Perimeter
Firewall
Inline
Sensor
1106
Solaris
NT
Mandrake
1106
2k
Hub
1104
1104
RedHat
Turbo
Solaris
98

FIG. 11

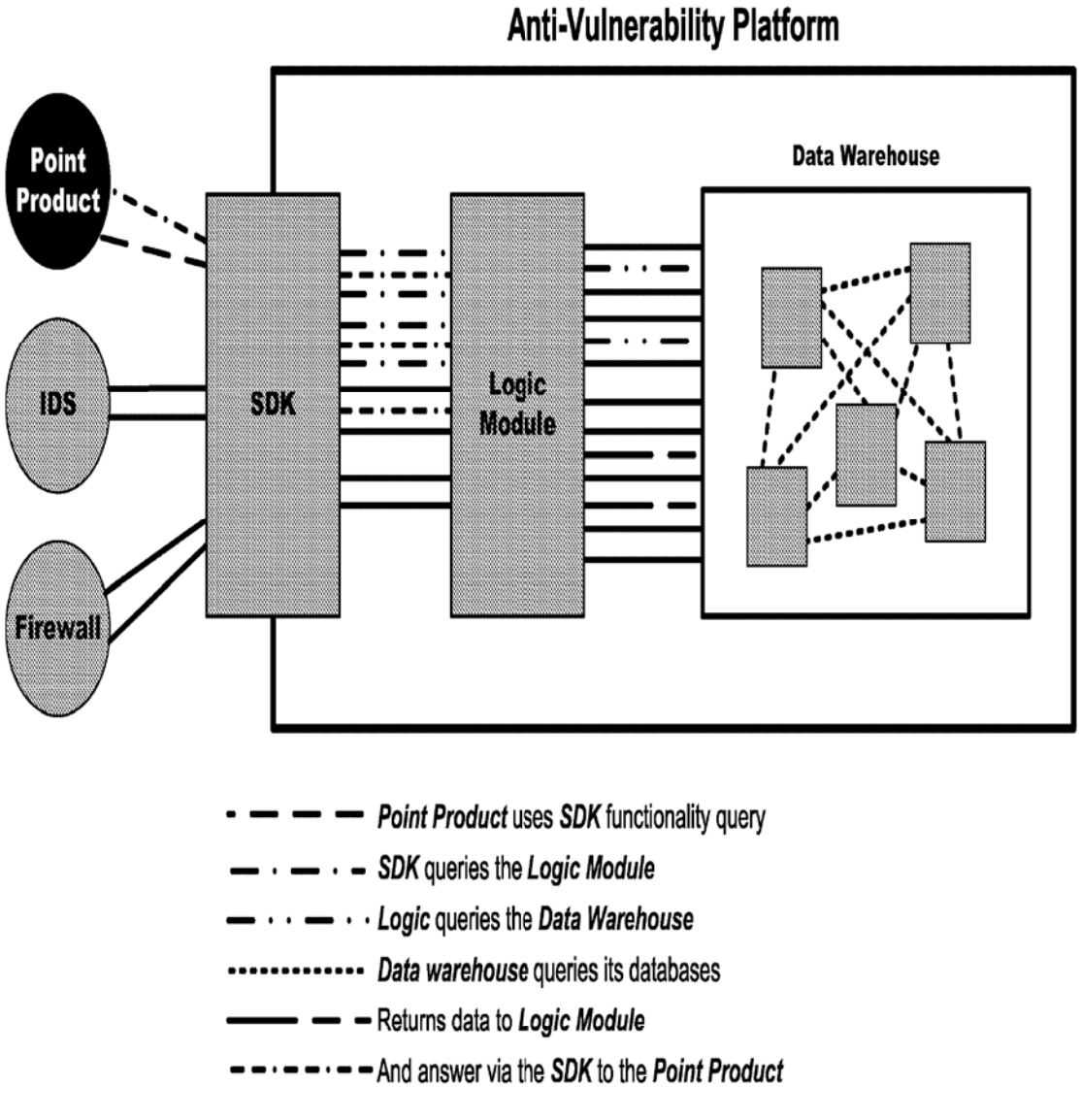

Anti-Vulnerability Platform
Point Product
IDS
Firewall
SDK
Logic Module
Data Warehouse
Point Product uses SDK functionality query
SDK queries the Logic Module
Logic queries the Data Warehouse
Data warehouse queries its databases
Returns data to Logic Module
And answer via the SDK to the Point Product

FIG. 12

Doc Code: PET.GLOSSARY
Document Description: Petition for Glossary Pilot

PTO/SB/436 (05-14)

CERTIFICATION AND PETITION TO MAKE SPECIAL UNDER THE GLOSSARY PILOT PROGRAM		
Attorney Docket Number: SP1P0012	Application Number (if known):	Filing date: 09-28-2014
First Named Inventor: Brett M. Oliphant		
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND PETITIONS TO PARTICIPATE IN THE GLOSSARY PILOT PROGRAM FOR THE ABOVE-IDENTIFIED APPLICATION.

1. This certification and petition is being electronically filed with the non-provisional application using the USPTO electronic filing system (EFS-Web).
2. The application is an original non-provisional utility application filed under 35 U.S.C. 111(a) within the duration of the pilot program. The following are excluded from the program: design applications, national stage applications, plant applications, PCT international applications, provisional applications, reissue applications, and reexamination proceedings.
3. The application cannot claim the benefit of a prior U.S. application except a provisional application, unless the application is a continuation-in-part application. All benefit claims are included in an application data sheet (see 37 CFR 1.76 and 1.78), and the applicable box is checked below:
   - ☐ a. This application does not directly claim the benefit of any prior U.S. application.
   - --- OR ---
   - ☐ b. This application directly claims the benefit of a provisional application filed within the previous 12 months.
   - --- OR ---
   - ☑ c. This application is a continuation-in-part application claiming the benefit of one or more prior U.S. or PCT international applications.
4. The application can claim priority to a foreign application, and all priority claims are included in an application data sheet (see 37 CFR 1.76 and 1.78). The applicable box is checked below:
   - ☑ a. This application does not claim priority to a foreign application.
   - --- OR ---
   - ☐ b. This application claims priority to one or more foreign applications. Copies of the foreign applications are being submitted herewith. If any of the foreign applications is not in the English language, an English-language translation of such foreign application is submitted herewith.
5. The application contains, or is amended to contain, at least one claim but no more than four (4) independent claims and thirty (30) total claims.
6. The application does not contain any multiple dependent claims.
7. By filing this certification and petition, applicant certifies that the application contains a glossary section in the Detailed Description, and that the glossary section meets all of the eligibility requirements for expedited examination until the first Office action under the Glossary Pilot Program. See Instruction Sheet.

Signature /Thomas D. Fortenberry/	Date 09-28-2014
Name (Print/Typed) Thomas D. Fortenberry	Registration Number 56537

Note: *This form must be signed in accordance with 37 CFR 1.33. Please see 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required - see below*.*

*Total of ___ forms are submitted.

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 14499230 Document Date: 09/28/2014

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://Score.uspto.gov/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/499,230

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	2 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/499,230	09/28/2014	2431	730	SP1P0012	2	1

CONFIRMATION NO. 9215

112117
Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

FILING RECEIPT

OC000000071094617

Date Mailed: 10/02/2014

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

Inventor(s)

Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

Applicant(s)

SecurityProfiling, LLC, Garland, TX

Power of Attorney: The patent practitioners associated with Customer Number 112117

Domestic Priority data as claimed by applicant

This application is a CIP of 14/138,014 12/21/2013
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/01/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/499,230**

Projected Publication Date: To Be Determined - pending completion of Corrected Papers

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

ForcePoint LLC
EX-1009
Page080

Title

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

ForcePoint LLC
EX-1009
Page081

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

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

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

ForcePoint LLC
EX-1009
Page082

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/499,230	09/28/2014	Brett M. Oliphant	SP1P0012

CONFIRMATION NO. 9215

112117
Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

FORMALITIES LETTER

OC000000071094618

Date Mailed: 10/02/2014

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. 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 required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application contains drawings, but the specification does not contain a brief description of the several views of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

The following item(s) appear to have been **omitted** from the application:

- Figure(s) **5A** described in the specification.

Applicant must reply to this notice within the time period set forth in this notice to avoid abandonment of this application. Applicant must select one of the three following options and the reply must comply with the requirements set forth in the selected option and any other requirements set forth in this notice. The reply should also indicate which option applicant has selected.

I. Petition for date of deposit: Should applicant contend that the above-noted omitted item(s) was in fact deposited in the U.S. Patent and Trademark Office (USPTO) with the nonprovisional application papers, a copy of this Notice and a petition (and the petition fee set forth in 37 CFR 1.17(f) with evidence of such deposit **must** be filed within **TWO MONTHS** of the date of this Notice. The petition fee will be refunded if it is determined that the item(s) was received by the USPTO. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).**

II. Petition for later filing date: Should applicant desire to supply the omitted item(s) and accept the date that such omitted item(s) was filed in the USPTO as the filing date of the above-identified application, a copy of this Notice, the omitted item(s), and a petition under 37 CFR 1.182 with the petition fee set forth in 37 CFR 1.17(f) requesting the later filing date **must** be filed within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).**

ForcePoint LLC
EX-1009
Page083

Applicant is advised that generally the filing fee required for an application is the filing fee in effect on the filing date accorded the application and that payment of the requisite basic filing fee on a date later than the filing date of the application requires payment of a surcharge (37 CFR 1.16(f)). To avoid processing delays and payment of a surcharge, applicant should submit any balance due for the requisite filing fee based on the later filing date being requested when submitting the omitted item(s) and the petition (and petition fee) requesting the later filing date.

III. Acceptance of application as deposited: Applicant may accept the application as deposited in the USPTO by filing an appropriate amendment as set forth in either (A) or (B) below within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b)** . The application will maintain a filing date as of the date of deposit of the application papers in the USPTO, and original application papers (i.e., the original disclosure of the invention) will include only those application papers present in the USPTO on the date of deposit. A petition is not required for this option.

(A) If applicant wants to accept the application as deposited without adding the subject matter that was in the omitted item (e.g., a missing page or figure), applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. For a missing page of the specification,
   a) a substitute specification including claims that amends the specification to renumber the pages consecutively and cancels any incomplete sentences, and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
2. For a missing figure of the drawings,
   a) replacement drawing sheets in compliance with 37 CFR 1.121(d) to renumber the drawing figures consecutively (if necessary),
   b) a substitute specification excluding claims that amends the specification to cancel any references to any omitted drawing(s) and corrects the references in the specification to the drawing figures to correspond with any relabeled drawing figures, and
   c) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
3. For a missing page of the claim listing only, a replacement claim listing with the claims renumbered consecutively or, if amendment to the claims is also necessary, then a complete claim listing in compliance with 37 CFR 1.121(c);
4. For a missing or unreadable compact disc,
   a) a substitute specification (excluding the claims) deleting the reference to the compact disc and the files contained on the compact disc, and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
5. For a missing or unreadable file submitted on a compact disc,
   a) a substitute specification (excluding the claims) deleting the reference to the missing or unreadable file, and a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
   b) a replacement transmittal letter listing all of the files except the missing or unreadable file in compliance with 37 CFR 1.52(e)(3)(ii).

(B) Alternatively, if applicant wants to accept the application as deposited but wishes to add the subject matter in the omitted item (e.g., a missing page or figure) by relying on an incorporation by reference under 37 CFR 1.57 or other portions of the original disclosure, applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. To add the subject matter in a missing page of specification,
   a) a substitute specification excluding claims and
   b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;

ForcePoint LLC
EX-1009
Page084

2. To add a missing figure of the drawings, new and replacement drawing sheets in compliance with 37 CFR 1.121(d);
3. To add the subject matter in a missing page of the claim listing, a complete claim listing in compliance with 37 CFR 1.121(c) (e.g., a claim in the missing page should be submitted as a new claim);
4. To add the subject matter in a missing or unreadable compact disc,
   a) a replacement compact disc and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
   b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4); and,
5. To add the subject matter in a missing or unreadable file submitted on a compact disc,
   a) a replacement compact disc that contains all of the files listed in the specification including the missing or unreadable file and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
   b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4).

If applicant is relying on an incorporation by reference under 37 CFR 1.57 to add the omitted subject matter, then applicant must also comply with the requirements of 37 CFR 1.57.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

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

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/aabranyos/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

ForcePoint LLC
EX-1009
Page085

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Oliphant et al. Application No.: 14/499,230 Filed: 09/28/2014 For: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Confirmation No.: 9215 Examiner: Unassigned Art Unit: 2431 Atty. Docket No.: SFC1P0012 Date: 10/17/2014

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

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

Sir:

In response to the Notice to File Corrected Application Papers, mailed 10/02/2014, Applicants hereby attach Replacement Sheet Figure 5A replacing Figure 5. In accordance with the Notice to File Corrected Application Papers, the Applicant elects option 3, Acceptance of Application as Deposited. Applicants believe a substitute specification is not necessary in view of the Replacement Sheet submitted herewith, which is described in the specification. No new matter has been added.

The Commissioner is authorized to charge any other fee(s) that may be due to our Deposit Account No. 50-6056.

Respectfully submitted,

/Thomas D. Fortenberry/

Thomas D. Fortenberry
Reg. No. 56,537

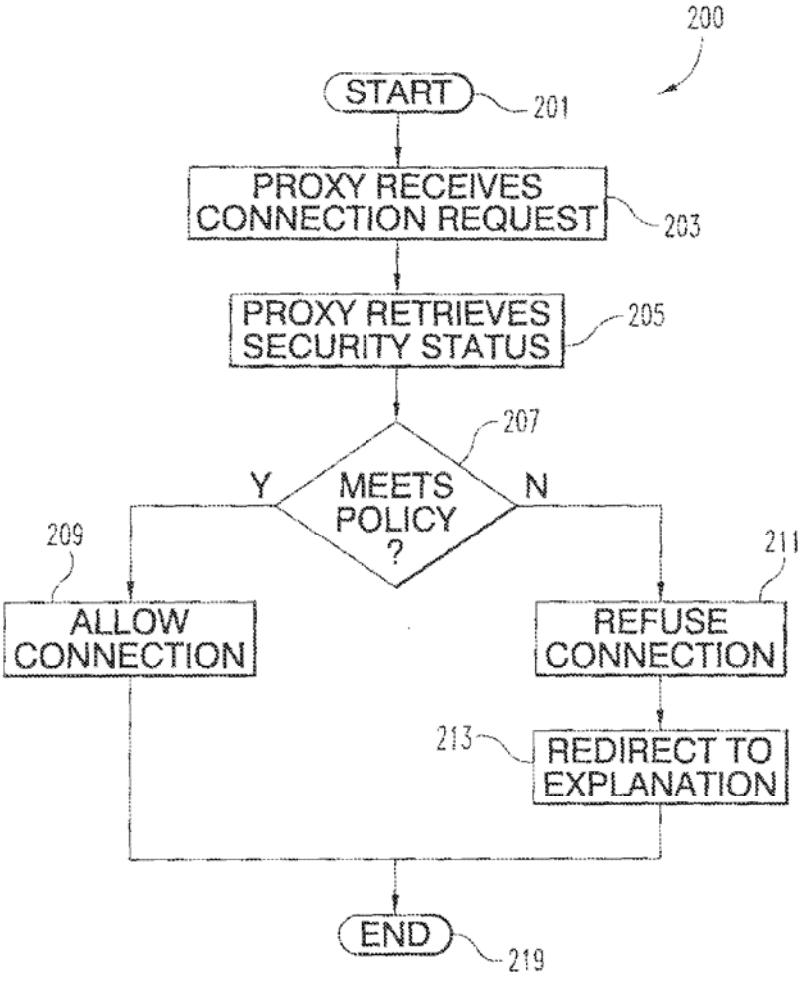

200
START
201
PROXY RECEIVES CONNECTION REQUEST
203
PROXY RETRIEVES SECURITY STATUS
205
207
MEETS POLICY ?
Y
N
209
ALLOW CONNECTION
211
REFUSE CONNECTION
213
REDIRECT TO EXPLANATION
END
219

FIG. 5A

Electronic Acknowledgement Receipt	
EFS ID:	20468569
Application Number:	14499230
International Application Number:	
Confirmation Number:	9215
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	112117
Filer:	THOMAS DONALD FORTENBERRY
Filer Authorized By:	
Attorney Docket Number:	SP1P0012
Receipt Date:	21-OCT-2014
Filing Date:	28-SEP-2014
Time Stamp:	02:19:52
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		SP1P0012_RespCorrectedAppPapers_10-17-2014.pdf	89297 d1a7504a436e2d8610987dddd4a0c705c5ff1e2ac	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Drawings-only black and white line drawings	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	89297	

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

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

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

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/499,230

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	2 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/499,230	09/28/2014	2431	730	SFC1P0012	2	1

CONFIRMATION NO. 9215

112117
Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

UPDATED FILING RECEIPT

OC000000071455150

Date Mailed: 10/22/2014

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

Inventor(s)

Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

Applicant(s)

SecurityProfiling, LLC, Garland, TX

Power of Attorney: The patent practitioners associated with Customer Number 112117

Domestic Priority data as claimed by applicant

This application is a CIP of 14/138,014 12/21/2013
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/01/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/499,230**

Projected Publication Date: Perfected

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

ForcePoint LLC
EX-1009
Page091

Title

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

ForcePoint LLC
EX-1009
Page092

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

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

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

ForcePoint LLC
EX-1009
Page093

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/499,230

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	2 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/499,230	09/28/2014	2431	730	SFC1P0012	2	1

CONFIRMATION NO. 9215

112117
Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

UPDATED FILING RECEIPT

OC000000071455150

Date Mailed: 10/27/2014

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

Inventor(s)

Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

Applicant(s)

SecurityProfiling, LLC, Garland, TX

Power of Attorney: The patent practitioners associated with Customer Number 112117

Domestic Priority data as claimed by applicant

This application is a CIP of 14/138,014 12/21/2013
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/01/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/499,230**

Projected Publication Date: 02/05/2015

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

ForcePoint LLC
EX-1009
Page095

Title

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

ForcePoint LLC
EX-1009
Page096

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

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

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

ForcePoint LLC
EX-1009
Page097

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.
14/499,230	09/28/2014	Brett M. Oliphant	SFC1P0012	9215

112117 7590 11/06/2014
Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

EXAMINER	
PRIETO, BEATRIZ	
ART UNIT	PAPER NUMBER
2400	
MAIL DATE	DELIVERY MODE
11/06/2014	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.

ForcePoint LLC
EX-1009
Page098

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/499,230	28 September, 2014	OLIPHANT ET AL.	SFC1P0012

Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

EXAMINER	
BEATRIZ PRIETO	
ART UNIT	PAPER
2400	20141031

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

This is a decision on the petition filed September 28, 2014 under 37 C.F.R. §1.102 to make the above-identified application special until the issuance of the first Office action under the Glossary Pilot Program as set forth in 79 Federal Register 17137 (March 27, 2014).

The petition to make special is before Technology Center (TC) 2400 Glossary Point of Contact for decision. The requirement for a fee for consideration of the petition to make special for applications in the Glossary Pilot Program has been waived.
The instant petition complies with the requirements of the Glossary Pilot Program as set forth in 79 Federal Register 17137.

Accordingly, the petition is GRANTED, and the above-identified application is accepted into the Glossary Pilot Program and will receive special status until the issuance of the first Office action.

Please note that as a condition of participation in this pilot program, any preliminary amendments that render the application non-compliant with the requirements of the Glossary Pilot Program will not be entered.

Telephone inquiries concerning this decision should be directed to Beatriz Prieto, Quality Assurance Specialist for TC 2400 at (571) 272-3902.

The application is being forwarded to TC 2400 for action on the merits commensurate with this decision.

/Beatriz Prieto/
Quality Assurance Specialist, TC 2400

PTO-90C (Rev.04-03)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Oliphant Application No.: 14/499,230 Filed: 09/28/2014 For: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Confirmation No.: 9215 Examiner: YALEW, FIKREMARIAM A Art Unit: 2436 Atty. Docket No.: SP1P0012 Date: 11/11/2014

PRELIMINARY AMENDMENT

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

Dear Sir:

Please enter the following amendments in advance of substantive prosecution:

ForcePoint LLC
EX-1009
Page100

AMENDMENT TO CLAIMS

1-2. (Cancelled)

3. (New) A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:

code for:

accessing at least one data storage identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, such that:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

code for:

displaying at least one mitigation technique in connection with at least one vulnerability to be applied as an attack response, and

receiving user input for selecting the at least one mitigation technique in connection with the at least one vulnerability; and

code for:

receiving information in connection with at least one of a plurality of devices, and

ForcePoint LLC
EX-1009
Page101

identifying a particular attack in connection with the at least one device that takes advantage of the at least one vulnerability, based on the information;

wherein the computer program product is operable such that, as a result of the user input for selecting the at least one mitigation technique in connection with the at least one vulnerability, the particular attack is prevented from taking advantage of the at least one vulnerability, while there is no update at the at least one of the device that removes the at least one vulnerability from the at least one device.

4. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the displayed at least one mitigation technique includes at least two mitigation techniques include a firewall option for preventing at least one attack packet of the particular by terminating or dropping the same, and an intrusion detection or prevention option for preventing a connection request; the computer program product is further operable such that, in response to user input received prior to the particular, the firewall option is capable of being applied to a plurality of different devices for preventing the at least one attack packet at any of the different devices; and the computer program product is further operable such that, in response to additional user input after the particular in connection with a particular single device of the plurality of different devices, the intrusion detection or prevention option is capable of being applied to the particular single device for preventing the connection request at the particular single device.

5. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the displayed at least one mitigation technique includes at least two mitigation techniques include a firewall option for preventing at least one attack packet of the particular by terminating or dropping the same, and an intrusion detection or prevention option for preventing a connection request; the computer program product is further operable such that, in response to user input prior to the particular in connection, the intrusion detection or prevention option is capable of being applied to a plurality of different devices for preventing the connection request at the plurality of

ForcePoint LLC
EX-1009
Page102

different devices; and the computer program product is further operable such that, in response to user input after the particular in connection with a particular single device of the plurality of different devices, the firewall option is capable of being applied to the particular single device for preventing the at least one attack packet at the particular single device.

6. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the at least one vulnerability is identified as a function of at least one of an operating system or an application identified in connection with a device, so that, in order to avoid false positives, only relevant vulnerabilities prompt mitigation technique user selection among at least two of the mitigation techniques, which involve both firewall and intrusion prevention system actions, for providing diverse mitigation options in connection with the particular.

7. (New) The computer program product of Claim 3, wherein the computer program product is operable such that which of the mitigation techniques that are displayed are based on actual vulnerabilities to which the at least one device is actually vulnerable so that only relevant mitigation techniques are displayed for selection by the user for real-time attack mitigation.

8. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the at least one vulnerability is identified as a function of at least one of an operating system or an application identified in connection with the at least one device and the at least one mitigation technique is specific to the at least one vulnerability, so that only relevant one or more vulnerabilities prompt selection of relevant one or more mitigation techniques by the user for application.

9. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the user input is capable of being received via at least one user interface for different devices, for allowing different attack mitigation actions including at least one intrusion prevention action and at least one firewall action to be

ForcePoint LLC
EX-1009
Page103

selectively applied to the different devices for different actual vulnerabilities determined to be actually relevant based on a presence of at least one of an operating system or an application.

10. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the displayed at least one mitigation technique includes at least two mitigation techniques including a first mitigation technique that utilizes a firewall action for at least mitigating the particular attack that takes advantage of the at least one vulnerability and a second mitigation technique that utilizes an intrusion prevention action for at least mitigating the particular attack that takes advantage of the at least one vulnerability.

11. (New) The computer program product of Claim 10, wherein the computer program product is operable such that different user input is capable of being received via at least one console for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by the user to the different devices for different actual vulnerabilities.

12. (New) The computer program product of Claim 10, wherein the computer program product is operable such that different user input is capable of being received via at least one console for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by the user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

13. (New) The computer program product of Claim 10, wherein the computer program product is operable such that the displayed at least one mitigation technique

ForcePoint LLC
EX-1009
Page104

further includes a third mitigation technique that utilizes a policy compliance action for at least mitigating the particular attack that takes advantage of the at least one vulnerability, wherein the computer program product is operable such that different user input is capable of being received via at least one console for different devices, for allowing different mitigation techniques including the first mitigation technique, the second mitigation technique, and the third mitigation technique to be selectively applied by the user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device, and the third mitigation technique being selectively applied by the user to the at least one first device, the at least one second device, and the at least one third device.

14. (New) The computer program product of Claim 10, wherein the computer program product is operable such that the first mitigation technique is automatically applied utilizing a first communication from a server to firewall-supporting client code, and the second technique is automatically applied utilizing a second communication from the server to intrusion prevention system-supporting client code, where the firewall-supporting client code and the system-supporting client code are part of the same client agent.

15. (New) The computer program product of Claim 10, wherein the computer program product is operable such that the first mitigation technique and the second technique are automatically applied by sending at least one encrypted communication from a server to an intrusion prevention system-supporting and firewall-supporting client code associated with the same single platform.

ForcePoint LLC
EX-1009
Page105

16. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the information is capable of being used to determine a characterization of a payload.

17. (New) The computer program product of Claim 3, wherein the computer program product is operable such that the at least one data storage identifies the plurality of mitigation techniques based on receipt of an identification of an operating system of the at least one device.

18. (New) The computer program product of Claim 17, wherein the computer program product is operable such that such that the particular attack is prevented from taking advantage of the at least one vulnerability which includes an actual vulnerability of the at least one device related to the operating system thereof.

19. (New) The computer program product of Claim 18, wherein the computer program product is operable such that the identification of the operating system of the at least one device is received as a result of a vulnerability assessment scan.

20. (New) The computer program product of Claim 3, wherein at least one of:

said at least one data storage includes at least one database;

said at least one data storage is accessed by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said mitigation techniques include remediation techniques;

each mitigation technique has a mitigation type including the patch;

each mitigation technique has a mitigation type including the policy setting;

each mitigation technique has a mitigation type including the configuration option;

each mitigation technique is capable of mitigating the effect of the attack that takes advantage of the corresponding vulnerability, by dropping packets associated with the attack or removing the corresponding vulnerability;

ForcePoint LLC
EX-1009
Page106

said information is capable of being used to determine an intended destination of a connection request; or

said information includes a vulnerability identifier;

wherein the computer program product is operable for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation technique; and wherein the computer program product is operable for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

21. (New) A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:

code for:

accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, such that:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

code for:

receiving information in connection with at least one of a plurality of devices; and

identifying an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information;

ForcePoint LLC
EX-1009
Page107

code for:

automatically applying at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device, in response to the attack for mitigating the attack;

wherein the computer program product is operable such that the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability, while there is no update at the at least one of the device that removes the at least one vulnerability from the at least one device.

22. (New) A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:

at least one data storage identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities associated with an operating system identified in connection with at least one of a plurality of devices, such that:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

code for:

displaying at least two of the mitigation techniques in connection with at least one vulnerability, and

ForcePoint LLC
EX-1009
Page108

receiving at least one user input in connection with the at least two mitigation techniques;

code for:

automatically applying the at least two mitigation techniques based on the user input, the at least two mitigation techniques including:

at least one first mitigation technique for utilizing a firewall for attack mitigation, and

at least one second mitigation technique for utilizing an intrusion prevention system for attack mitigation; and

code for:

receiving information in connection with the at least one device, and

identifying a particular attack in connection with the at least one device that takes advantage of the at least one vulnerability, based on the information;

wherein the computer program product is operable such that the attack is mitigated utilizing the first mitigation technique for utilizing the firewall for attack mitigation and the at least one second mitigation technique for second mitigation technique for utilizing the intrusion prevention system for attack mitigation, regardless of whether there is no update at the at least one of the device that removes the at least one vulnerability from the at least one device.

ForcePoint LLC
EX-1009
Page109

REMARKS

Applicant has clarified what is claimed. No claim is intended to invoke 35 U.S.C. 112, paragraph 6. It is believed that no fees are due in connection with this filing.

Respectfully submitted,

/Brian Owens/

Brian Owens
Reg. No. 55,517

Brian Owens, Esq.
3712 Kimble Dr.
Plano, TX 75025
(469) 235-4750
patentfacilitator@gmail.com

ForcePoint LLC
EX-1009
Page110

Electronic Acknowledgement Receipt	
EFS ID:	20669259
Application Number:	14499230
International Application Number:	
Confirmation Number:	9215
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	112117
Filer:	Brian Dean Owens
Filer Authorized By:	
Attorney Docket Number:	SP1P0012
Receipt Date:	12-NOV-2014
Filing Date:	28-SEP-2014
Time Stamp:	03:03:41
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	Power of Attorney	SP1P0012_POA.pdf	202871 54644301fb032dd13e4876883d437dffb5d2c0ab	no	2
Warnings:					
Information:					

2	Preliminary Amendment	SP1P0012_Preliminary_Amendment_11_11_2014.pdf	364267 91cd414763c965b9d86398fd54b350f6248c30b1	no	11
Warnings:					
Information:					
			Total Files Size (in bytes):	567138	

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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	14/499,230
Filing Date	09-28-2014
First Named Inventor	Brett M. Oliphant
Title	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
Art Unit	2436
Examiner Name	YALEW, FIKREMARIAM A
Attorney Docket Number	SP1P0012

SIGNATURE of Applicant or Patent Practitioner

Signature	/Brian Owens/	Date (Optional)	
Name	Brian Owens	Registration Number	55,517
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 2 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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 BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 127962

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

SecurityProfiling, LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/John Blignaut/	Date (Optional)	
Name	John Blignaut		
Title	Member - SecurityProfiling, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Best Available Copy

Approved for use through 1/31/2014. 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 14/499,230	Filing Date 9/28/14	☐ To be Mailed

ENTITY ☐ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE	N/A	N/A	N/A	
☐ SEARCH FEE	N/A	N/A	N/A	
☐ EXAMINATION FEE	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =		x $	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =		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 $310 ($155 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	

APPLICATION AS AMENDED – PART II

AMENDMENT	11/12/14	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x $	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x $	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						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.

Angelina Tubbs

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.

ForcePoint LLC
EX-1009
Page115

Doc Code: FAI.REQ
Document Description: Request First Action Interview

PTO/SB/413C (05-11)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U. S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR FIRST ACTION INTERVIEW (FULL PILOT PROGRAM)

Attorney Docket Number: SP1P0012	Application Number (if known): 14/499,230	Filing date: 09-28-2014
First Named Inventor: Brett M. Oliphant	Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

APPLICANT HEREBY REQUESTS A FIRST ACTION INTERVIEW IN THE ABOVE-IDENTIFIED APPLICATION. See Instruction Sheet on page 2.

1. The application must contain three (3) or fewer independent claims and twenty (20) or fewer total claims.

2. The application must not contain any multiple dependent claims.

3. By filing this request:

   Applicant is agreeing to make an election without traverse if the Office determines that the claims are not obviously directed to a single invention; and

   Applicant is agreeing not to request for a refund of the search fee and any excess claims fee paid in the application after the mailing or notification of the pre-interview communication prepared by the examiner.

4. Other attachments: _____

Signature /Brian Owens/	Date 11/14/2014
Name (Print/Typed) Brian Owens	Registration Number 55,517

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

■ *Total of 1 forms are submitted.

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 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, 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.

Doc Code: FAI.REQ
Document Description: Request First Action Interview

PTO/SB/413C (05-11)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U. S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR FIRST ACTION INTERVIEW (FULL PILOT PROGRAM)

Attorney Docket Number: SP1P0012	Application Number (if known): 14/499,230	Filing date: 09-28-2014
First Named Inventor: Brett M. Oliphant	Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

APPLICANT HEREBY REQUESTS A FIRST ACTION INTERVIEW IN THE ABOVE-IDENTIFIED APPLICATION. See Instruction Sheet on page 2.

1. The application must contain three (3) or fewer independent claims and twenty (20) or fewer total claims.

2. The application must not contain any multiple dependent claims.

3. By filing this request:

   Applicant is agreeing to make an election without traverse if the Office determines that the claims are not obviously directed to a single invention; and

   Applicant is agreeing not to request for a refund of the search fee and any excess claims fee paid in the application after the mailing or notification of the pre-interview communication prepared by the examiner.

4. Other attachments: _____

Signature /Brian Owens/	Date 11/14/2014
Name (Print/Typed) Brian Owens	Registration Number 55,517

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

■ *Total of 1 forms are submitted.

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 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, 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.

Electronic Acknowledgement Receipt	
EFS ID:	20704552
Application Number:	14499230
International Application Number:	
Confirmation Number:	9215
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	112117
Filer:	Brian Dean Owens
Filer Authorized By:	
Attorney Docket Number:	SP1P0012
Receipt Date:	14-NOV-2014
Filing Date:	28-SEP-2014
Time Stamp:	16:39:36
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	First Action Interview - Enrollment Request	SP1P0012_Interview_Pilot_Program_11-14-14_Signed.pdf	569142 811312f644eeb425a8a1075c7b2831c4d9c6d37	no	1

Warnings:
Information:

Total Files Size (in bytes):	569142

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/499,230	09/28/2014	Brett M. Oliphant	SP1P0012

CONFIRMATION NO. 9215

127962
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

POA ACCEPTANCE LETTER

OC000000071898742

Date Mailed: 11/20/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/12/2014.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/zabraha/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

ForcePoint LLC
EX-1009
Page120

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/499,230	09/28/2014	Brett M. Oliphant	SP1P0012

CONFIRMATION NO. 9215

112117
Thomas D. Fortenberry, Attorney at Law
P.O. Box 2099
Woodville, TX 75979

POWER OF ATTORNEY NOTICE

OC000000071898632

Date Mailed: 11/20/2014

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/12/2014.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/zabraha/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

ForcePoint LLC
EX-1009
Page121

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	14499230
Filing Date	2014-09-28
First Named Inventor	Brett M. Oliphant
Art Unit	2436
Examiner Name	YALEW, FIKREMARIAM A
Attorney Docket Number	SP1P0012

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5008814		1991-04-16	Mathur	
	2	5253932		1993-10-19	Nesovic	
	3	5335346		1994-08-02	Fabbio	
	4	5683638		1997-11-04	Crigler et al.	
	5	5765153		1998-06-09	Benantar et al.	
	6	5892903		1999-04-06	Klaus	
	7	5991881		1999-11-23	Conklin et al.	
	8	6005942		1999-12-21	Chan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	9	6044466		2000-03-28	Anand et al.	
	10	6074727		2000-06-13	Miller et al.	
	11	6131163		2000-10-10	Wiegel	
	12	6185689		2001-02-06	Todd Sr. et al.	
	13	6219786		2001-04-17	Cunningham et al.	
	14	6282546		2001-08-28	Gleichauf et al.	
	15	6298445		2001-10-02	Shostack et al.	
	16	6321334		2001-11-20	Jerger et al.	
	17	6324656		2001-11-27	Gleichauf et al.	
	18	6345361		2002-02-05	Jerger et al.	
	19	6418554		2002-07-09	Delo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	20	6473800		2002-10-29	Jerger et al.	
	21	6526513		2003-02-25	Shrader et al.	
	22	6754896		2004-06-22	Mishra et al.	
	23	6816896		2004-11-09	Fortin et al.	
	24	6966059		2005-11-15	Shetty et al.	
	25	6990591		2006-01-24	Pearson	
	26	7000247		2006-02-14	Banzhof	
	27	7010696		2006-03-07	Cambridge et al.	
	28	7051097		2006-05-23	Pecina	
	29	7051365		2006-05-23	Bellovin	
	30	7076801		2006-07-11	Gong et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	31	7080141		2006-07-18	Baekelmans et al.	
	32	7159237		2007-01-02	Schneier et al.	
	33	7178144		2007-02-13	Melchione et al.	
	34	7216343		2007-05-08	Das et al.	
	35	7228566		2007-06-05	Caceres et al.	
	36	7240193		2007-07-03	Hatfalvi et al.	
	37	7278163		2007-10-02	Banzhof et al.	
	38	7308712		2007-12-11	Banzhof	
	39	7315801		2008-01-01	Dowd et al.	
	40	7353539		2008-04-01	Brawn et al.	
	41	7424706		2008-09-09	Ivanov et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	42	7458098		2008-11-25	Judge et al.	
	43	7509676		2009-03-24	Trueba	
	44	7519954		2009-04-14	Beddoe et al.	
	45	7519994		2009-04-14	Judge et al.	
	46	7536456		2009-05-19	Williams et al.	
	47	7624422		2009-11-24	Williams et al.	
	48	7627891		2009-12-01	Williams et al.	
	49	7673043		2010-03-02	Keir et al.	
	50	7698275		2010-04-13	O'Brien et al.	
	51	7761920		2010-07-20	Bezilla et al.	
	52	7827607		2010-11-02	Sobel et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	53	7836501		2010-11-16	Sobel et al.	
	54	7882555		2011-02-01	Ben-Itzhak	
	55	8091117		2012-01-03	Williams et al.	
	56	8135823		2012-03-13	Cole et al.	
	57	8135830		2012-03-13	McClure et al.	
	58	8181173		2012-05-15	Childress et al.	
	59	8185930		2012-05-22	Alperovitch et al.	
	60	6952779		2005-10-04	Cohen et al.	
	61	6957348		2005-10-18	Flowers et al.	
	62	7073198		2006-07-04	Flowers et al.	
	63	7181769		2007-02-20	Keanini et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	64	7249187		2007-07-24	Sobel et al.	
	65	7562388		2009-07-14	Hackenberger et al.	
	66	7574740		2009-08-11	Kennis	
	67	7594273		2009-09-22	Keanini et al.	
	68	7779468		2010-08-17	Magdych et al.	
	69	7913303		2011-03-22	Rouland et al.	
	70	7954159		2011-05-31	Hrabik et al.	
	71	8121874		2012-02-21	Guheen et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010034847	A1	2001-10-25	GaulJr. Stephen E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	2	20020013811	A1	2002-01-31	Kim In-Gwang	
	3	20020026591	A1	2002-02-28	Hartley Bruce V. et al.	
	4	20020104014	A1	2002-08-01	Zobel Robert David et al.	
	5	20020112179	A1	2002-08-15	Riordan James F. et al.	
	6	20020199122	A1	2002-12-26	Davis Lauren B. et al.	
	7	20030005178	A1	2003-01-02	Hemsath David Kurt	
	8	20030014669	A1	2003-01-16	Caceres Maximiliano Gerardo et al.	
	9	20030037601	A1	2003-02-27	Mansky Paul et al.	
	10	20030061506	A1	2003-03-27	Cooper Geoffrey et al.	
	11	20030084320	A1	2003-05-01	Tarquini Richard Paul et al.	
	12	20030126472	A1	2003-07-03	Banzhof Carl E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	13	20030135749	A1	2003-07-17	Gales George S. et al.	
	14	20030145228	A1	2003-07-31	Suuronen Janne et al.	
	15	20040030778	A1	2004-02-12	Kronenberg Sandy Craig et al.	
	16	20040054764	A1	2004-03-18	Aderton Harry et al.	
	17	20040088565	A1	2004-05-06	Norman Andrew Patrick et al.	
	18	20040103310	A1	2004-05-27	Sobel William E. et al.	
	19	20040117640	A1	2004-06-17	Chu Simon C. et al.	
	20	20040243603	A1	2004-12-02	Komatsu Masaki	
	21	20050010819	A1	2005-01-13	Williams John Leslie et al.	
	22	20050015382	A1	2005-01-20	Aaron Jeffrey A.	
	23	20050033988	A1	2005-02-10	Chandrashekhar Ganesan et al.	

ForcePoint LLC
EX-1009
Page130

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	24	20050222969	A1	2005-10-06	Yip Ying-Kin Tony et al.	
	25	20050235360	A1	2005-10-20	Pearson Sterling Michael	
	26	20060265708	A1	2006-11-23	Blanding Stephen M. et al.	
	27	20070016659	A1	2007-01-18	Peck Joseph E. et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	EP1294128	EP	A1	2003-03-19	Motoyama et al.		☐
	2	JP2002366525	JP	A	2002-12-20	Koshida et al.		☐
	3	WO0214987	WO	A2	2002-02-21	Gadish et al.		☐
	4	WO03007192	WO	A1	2003-01-23	Caceres et al.		☐
	5	WO03029940	WO	A2	2003-04-10	Singleton et al.		☐

ForcePoint LLC
EX-1009
Page131

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	6	WO03029941	WO	A2	2003-04-10	Singleton et al.		☐
	7	WO2004086168	WO		2004-10-07	Moshir et al.		☐
	8	WO2004114663	WO		2004-12-29	Patel, Dipan		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	U.S. Provisional Application No. 60/448,313, filed February 14, 2003	☐
	2	"Symantec unveils vulnerability assessment tool," May 13, 2003, retrieved from https://web.archive.org/web/20140818164413/http://www.computerweekly.com/news/2240050753/Symantec-unveils-vulnerability-assessment-tool	☐
	3	Symantec Corporation, " Symantec Introduces New Vulnerability Assessment Solution: Symantec Vulnerability Assessment Provides Vulnerability Identification and Prioritization to Proactively Secure Systems at Risk, News Release, May 12, 2003, retrieved from http://www.symantec.com/press/2003/n030512a.html	☐
	4	"Introduction to Symantec Vulnerability Assessment 1.0," January 1, 2003, retrieved from "http://www.symantec.com/business/support/index?page=content&id=TECH111970	☐
	5	GULA, Ron, "Correlating IDS Alerts with Vulnerability Information," December 2002 (Updated January 2009), pp. 1-10, retrieved from http://docs.huihoo.com/nessus/va-ids.pdf	☐
	6	DESAI, Neil, "IDS Correlation of VA Data and IDS Alerts," June 29, 2003, retrieved from http://www.symantec.com/connect/articles/ids-correlation-va-data-and-ids-alerts	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	7	"Qualys Introduces First Network Vulnerability Assessment Platform for Managed Security and Consulting Organizations," April 10, 2001, retrieved from http://www.qualys.com/company/newsroom/news-releases/usa/2001-04-10-3/	☐
	8	"Qualys Introduces New Intranet Scanner Appliance," September 30, 2002, retrieved from http://www.qualys.com/company/newsroom/news-releases/usa/2002-09-30/	☐
	9	QUALYS "CASE STUDY: Bank of the West — Major Financial Institution Protects Information Assets Through Regular Network Vulnerability Audits," July 2005, retrieved from http://www.qualys.com/docs/bank_of_west.pdf	☐
	10	GULA, Ron, "Example Lightning Deployment Scenarios," December 2002, 5 pages, retrieved from https://web.archive.org/web/20030316012821/http://www.tenablesecurity.com/example.pdf	☐
	11	GULA, Ron, "Offering Managed Security Services with Lightning," December 2002, 6 pages, retrieved from https://web.archive.org/web/20030316085246/http://www.tenablesecurity.com/manage.pdf	☐
	12	Tenable Network Security Inc., "LIGHTNING CONSOLE," 2002, retrieved from https://web.archive.org/web/20030416093233/http://www.tenablesecurity.com/console.html	☐
	13	Tenable Network Security Inc., "Screen Shots," 2002, retrieved from https://web.archive.org/web/20030214013753/http://www.tenablesecurity.com/screenshots.html	☐
	14	SecurityProfiling, "News," July 2001, retrieved from https://web.archive.org/web/20021209114707/http://securityprofiling.com/news.htm	☐
	15	Symantec Corporation, "Norton Ghost™ User's Guide," 2002, 221 pages	☐
	16	Symantec Corporation, "Symantec™ Vulnerability Assessment Implementation Guide," Version 1.0, 2003, 108 pages	☐
	17	HUBER, Robert, "Strategies for Improving Vulnerability Assessment Effectiveness in Large Organizations," SANS Institute InfoSec Reading Room, Version 1.4b (amended August 29, 2002), GSEC Option 1, April 20, 2003, 18 pages	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

	18	U.S. Provisional Application No. 60/441,422, filed January 21, 2003	☐
	19	U.S. Provisional Application No. 60/388,078, filed June 11, 2002	☐
	20	U.S. Provisional Application No. 60/345,689, filed December 31, 2001	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14499230
	Filing Date	2014-09-28
	First Named Inventor	Brett M. Oliphant
	Art Unit	2436
	Examiner Name	YALEW, FIKREMARIAM A
	Attorney Docket Number	SP1P0012

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Brian Owens/	Date (YYYY-MM-DD)	2014-12-04
Name/Print	Brian Owens	Registration Number	55,517

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 294 128 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.03.2003 Bulletin 2003/12

(51) Int Cl.[7]: **H04L 12/26**, H04L 12/58, G06F 11/34, G06F 17/60

(21) Application number: **02020472.3**

(22) Date of filing: **12.09.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **17.09.2001 US 953358**

(71) Applicant: **Ricoh Company**
Tokyo 143-8555 (JP)

(72) Inventors:
- **Motoyama, Tetsuro**
  San Jose, CA 95131-1817 (US)
- **Fong, Avery**
  San Jose, CA 95131-1817 (US)

(74) Representative: **Schwabe - Sandmair - Marx**
Stuntzstrasse 16
81677 München (DE)

(54) Remote monitoring of network devices by means of e-mail messages

(57) A system, method, and computer program product for transferring monitoring information from a remote monitor (266,272,282) to a central monitor (254) responsible for monitoring devices on multiple networks. In a monitoring system for network devices is disclosed. A communication link is established between a remote monitor and a message transfer server (943). Monitoring information is formatted into a standard format, encrypted, encoded, and sent from the remote monitor to the central monitor as an attachment to an e-mail via the communication link to the message transfer server.

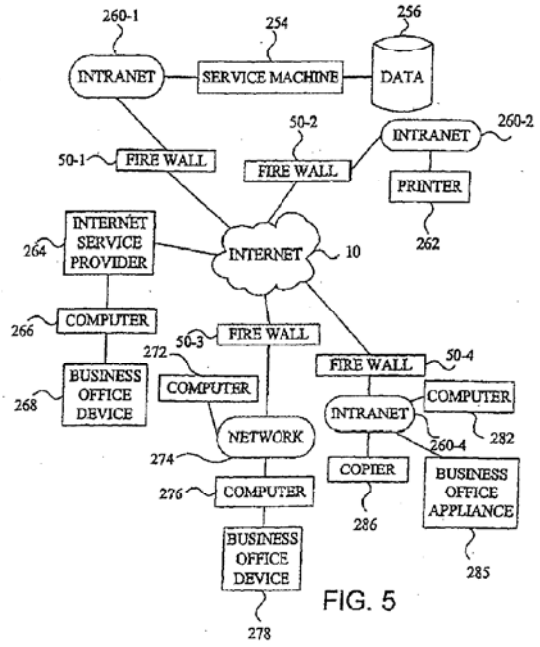


FIG. 5

EP 1 294 128 A1

Printed by Jouve, 75001 PARIS (FR)

ForcePoint LLC
EX-1009
Page137

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is related to U.S. Patent Application 09/190,460, filed November 13, 1998, entitled "Method and System for Translating Documents Using Different Translation Resources for Different Portions of the Documents," which is a continuation of U.S. Patent Application 08/654,207, filed May 28, 1996, entitled "Method and System for Translating Documents Using Different Translation Resources for Different Portions of the Documents," now U.S.P. 5,848,386; U.S. Patent Application 08/997,705, filed December 23, 1997, entitled "Object-oriented System and Computer Program Product for Mapping Structured Information to Different Structured Information," now U.S.P. 6,085,196; U. S. Patent Application 08/997,705, filed December 23, 1997, entitled "Method and Apparatus for Providing a Graphical User Interface for Creating and Editing a Mapping of a First Structural Description to a Second Structural Description"; US Patent Application 09/756,120, filed January 9, 2001, entitled "Method and System of Remote Support Of Device Using Email"; U.S. Patent Application 09/668,162, filed September 25, 2000, entitled "Method and System of Data collection and Mapping From a Remote Position Reporting Device"; U.S. Patent Application 09/575,710, filed July 25, 2000, entitled "Method and System of Remote Diagnostic and Information Collection and Service System"; U.S. Patent Application 09/575,702, filed July 12, 2000, entitled "Method and System of Remote Position Report Device"; U.S. Patent Application 09/453,934, filed May 17, 2000, entitled "Method and System of Remote Diagnostic, Control and Information Collection Using a Dynamic Linked Library for Multiple Formats and Multiple Protocols"; U.S. Patent Application 09/453,935, filed May 17, 2000, entitled "Method and System of Remote Diagnostic, Control and Information Collection Using a Dynamic Linked Library of Multiple Formats and Multiple Protocols With Intelligent Protocol Processor"; U.S. Patent Application 09/453,937, filed May 17, 2000, entitled "Method and System of Remote Diagnostic, Control and Information Collection Using a Dynamic Linked Library of Multiple Formats and Multiple Protocols With Restriction on Protocol"; U.S. Patent Application 09/453,936, filed May 17, 2000, entitled "Method and System of Remote Diagnostic, Control and Information Collection Using a Dynamic Linked Library of Multiple Formats and Multiple Protocols with Intelligent Formatter"; U.S. Patent Application 09/542,284, filed April 4, 2000, entitled "System and Method to Display Various Messages While Performing the Tasks or While Idling"; U.S. Patent Application 09/520,368, filed on March 7, 2000, entitled "Method and System for Updating the Device Driver of a Business Office Appliance"; U.S. Patent Application 09/453,877, filed February 4, 2000, entitled "Method and System for Maintaining a Business Office Appliance through Log Files"; U.S. Patent Application 09/440,692, filed November 16, 1999, entitled "Method and System to Monitor the Application Usage and Send Back the Information Using Connection and Connectionless Mode"; U.S. Patent Application 09/440,693, filed November 16, 1999, entitled "Method and System of Remote Diagnostic, Control and Information Collection Using a Dynamic Linked Library"; U.S. Patent Application 09/440,647, filed November 16, 1999, entitled "Method and System to Monitor the Application Usage and Send Back the Information Using Connection and Connectionless Mode"; U.S. Patent Application 09/440,646, filed November 16, 1999, entitled "Method and System to Monitor the Application Usage and Send Back the Information Using Connection and Connectionless Mode"; U.S. Patent Application 09/440,645, filed November 16, 1999, entitled "Application Unit Monitoring and Reporting System and Method With Usage Data Logged Into a Map Structure"; U.S. Patent Application 09/408,443, filed September 29, 1999, entitled "Method and System for Remote Diagnostic, Control, and Information Collection Based on various Communication Modes for Sending Messages to a Resource Manager"; U.S. Patent Application 09/407,769, filed September 29, 1999, entitled "Method and System for Remote Diagnostic, Control and Information Collection Based on various Communication Modes for Sending Messages to Users"; U.S. Patent Application 09/393,677, filed September 10, 1999, entitled "Application Unit Monitoring and Reporting System and Method"; U.S. Patent Application 09/311,148, filed May 13, 1999, entitled "Application Unit Monitoring and Reporting System and Method"; U.S. Patent Application 09/192,583, filed November 17, 1998, entitled "Method and System for Communicating With a Device Attached to a Computer Using Electronic Mail Messages"; U.S. Patent Application 08/883,492, filed June 26, 1997, entitled "Method and System for Diagnosis and Control of Machines Using Connectionless Modes Having Delivery Monitoring and an Alternate Communication Mode"; U.S. Patent Application 08/820,633, filed March 19, 1997, entitled "Method and System to Diagnose a Business Office Device Based on Operating Parameters Set by a User," now U.S.P. 5,887,216; U.S. Patent Application 08/733,134, filed October 16, 1996, entitled "Method and System for Diagnosis and Control of Machines Using Connectionless Modes of Communication," now U.S.P. 5,909,493; U.S. Patent Application 08/880,683, filed June 23, 1997, U.S. Patent Applications 09/107,989 and 09/108,705, both of which were filed July 1, 1998, all three of which are entitled "Method and System for Controlling and Communicating with Machines Using Multiple Communication Formats," and all three of which are divisions of U.S. Patent Application 08/624,228, filed March 29, 1996, entitled "Method and System for Controlling and Communicating with Machines Using Multiple Communication Formats," now U.S.P. 5,818,603; U.S. Patent Application 09/457,669, entitled "Method and System for Diagnosis and Control of Machines Using Connection and Connectionless Modes of Communication, " filed December 9, 1999, which is a continuation of U.S. Patent Application 08/916,009, entitled "Method and System

ForcePoint LLC
EX-1009
Page138

for Diagnosis and Control of Machines Using Connection and Connectionless Modes of Communication, " filed August 21, 1997, which is a continuation of U.S. Patent Applications 08/738,659 and 08/738,461, filed October 30, 1996, both of which are entitled "Method and System for Diagnosis and Control of Machines Using Connection and Connectionless Modes of Communication," which are divisions of U.S. Patent Application 08/463,002, filed June 5, 1995, entitled "Method and System for Diagnosis and Control of Machines Using Connection and Connectionless Modes of Communication", now U.S.P. 5,819,110; U.S. Patent. Application 08/852,413, filed May 7, 1987, entitled "Method and System for Controlling and Communicating with Business Office Devices," now U.S.P. 5,774,678, which is a continuation of U.S. Patent Application 08/698,068, filed August 15, 1996, entitled "Method and Apparatus for Controlling and Communicating With Business Office Devices", now U.S.P. 5,649,120, which is a continuation of U.S. Patent Application 08/562,192, filed November 22, 1995, now U.S.P. 5,568,618, entitled "Method and Apparatus for Controlling and Communicating With Business Office Devices", which is a continuation of U.S. Patent Application 08/473,780, filed June 6, 1995, entitled "Method and Apparatus for Controlling and Communicating With Business Office Devices", now U.S. P. 5,544,289, which is a continuation of U.S. Patent Application 08/426,679, filed April 24, 1995, entitled "Method and Apparatus for Controlling and Communicating With Business Office Devices," now U.S.P. 5,537,554, which is a continuation of U.S. Patent Application 08/282,168, filed July 28, 1994, entitled "Method and Apparatus for Controlling and Communicating With Business Office Devices", now U.S. Patent 5,412,779, which is a continuation of U.S. Patent Application 07/902,462, filed June 19, 1992, now abandoned, which is a continuation of U.S. Patent Application 07/549,278, filed July 6, 1990, now abandoned; U.S. Patent Application XX/XXX,XXX, filed XXX XX, 2001, entitled "SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR SENDING REMOTE DEVICE CONFIGURATION INFORMATION TO A MONITOR USING E-MAIL" (Attorney Docket Number 205847US-5244-5244-2); and U.S. Patent Application XX/XXX,XXX, filed XXX XX, 2001, entitled "SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR SENDING PERSISTENT AND NON-PERSISTENT STATUS INFORMATION TO A MONITOR USING E-MAIL" (Attorney Docket Number 205828US-5244-5244-2), the entire contents of each of these applications and patents are incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention:

[0002] This invention relates to systems, methods, and computer program products for monitoring networked devices. Configuration and status information is gathered from the networked devices by a remote monitor and is sent in an electronic mail form, such as e-mail, to a central monitoring site.

Discussion of the Background:

[0003] Co-pending U.S. patent application Serial No. 09/756,120 filed on January 09, 2001, describes a system for remotely monitoring networked devices using e-mail. As described in that application, the Simple Network Management Protocol (SNMP) is used by a remote monitor to collect information from networked devices. The collected information is then sent to a central monitor using, for example, e-mail.

[0004] In order to remotely monitor devices, both configuration information and status information are collected. Accordingly, as described in the above-referenced application, both configuration and status information are sent from the remote monitor to the central monitor. The configuration information may include, for example, device make and model information, device-unique serial number and address information, device physical location information, contact information, etc. The status information may include any number of alarm and state conditions depending on the type of device. For example, a printer may include a "paper jam" indicator, or an "out of paper" indicator, etc., while a business office appliance may include other indicators.

[0005] As the number of different classes of information (e.g., configuration or status) increases, or the number of different types of devices being supported increases, the complexity of remotely monitoring these devices also increases.

SUMMARY OF THE INVENTION

[0006] The inventors of the present invention have recognized that it would be advantageous to have a simple interface for transferring information using a commonly available resource in a system for remotely monitoring networked devices. The present inventors have further recognized that it would be advantageous to have an extensible data transfer capability that supports the transfer of different classes of information, for example, configuration information or status information, using a commonly available resource such as Internet e-mail. Moreover, the present inventors have recognized that it would be further advantageous if the transfer capability could be customized or extended without

ForcePoint LLC
EX-1009
Page139

impacting a small set of public methods used to implement a core set of functionality supported by the data transfer capability.

[0007] The present invention provides a system, method, and computer program product through which different classes of information are transferred from a remote monitor to a central monitor using, for example, Internet e-mail as a transfer mechanism. By having a simple interface, the complexities of performing the data transfer are hidden from applications using the data transfer mechanism. The present invention provides a data transfer capability that can be extended to include further capabilities, such as, for example, an encryption capability, without impacting the simple interface, and without impacting the ability to make use of a commonly available transfer mechanism, such as Internet e-mail.

[0008] In one embodiment, the data transfer capability of the present invention makes use of the commonly-available Internet e-mail as a transfer mechanism, and its capabilities are available through a public interface that includes a small set of functions. Through this small set of functions, a communication link between a remote monitor and a central monitor may be established, and information may be transferred from the remote monitor to the central monitor via Internet e-mail. The information that is sent may be either configuration information or status information. The same four methods are used irrespective of the type of information that is being transferred, thereby providing for ease in integration of the data transfer capability of the present invention.

[0009] The data transfer mechanism has been designed to be extensible without impacting the small set of functions that make up the public interface described above. For example, an abstract class has been provided through which encryption capabilities may be added. New derived classes of this abstract class can be added to support application-specific encryption needs. Any complexity added by a custom encryption capability is hidden from the public interface, and therefore will not impact the application making use of the data transfer mechanism.

[0010] One advantage of the present invention is that as more types of microprocessor-based devices become available, the data transfer capability of the present invention can be easily adapted to support these devices. The present invention provides an extensible capability that supports sending different classes of information using a commonly-available transport mechanism with a small set of functions making up the public interface. Furthermore, as the commonly-available transport mechanisms are improved, or replaced by superior capabilities, the simple public interface will continue to apply, and, therefore, can be taken advantage of without the need to modify the applications using the data transfer capability of the present invention.

[0011] Consistent with the title of this section, the above summary is not intended to be an exhaustive discussion of all the features or embodiments of the present invention. A more complete, although not necessarily exhaustive, description of the features and embodiments of the invention is found in the section entitled "DESCRIPTION OF THE PREFERRED EMBODIMENTS."

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

Figure 1 illustrates three networked business office devices connected to a network of computers and databases through the Internet;
Figure 2 illustrates the components of a digital image forming apparatus;
Figure 3 illustrates the electronic components of the digital image forming apparatus illustrated in Figure 2;
Figure 4 illustrates details of a multi-port communication interface illustrated in Figure 3;
Figure 5 illustrates an alternative system configuration in which business office devices are either connected directly to the network or connected to a computer which is connected to the network;
Figure 6A is a block diagram illustrating a flow of information to and from an application unit using electronic mail;
Figure 6B illustrates an alternative way of communicating using electronic mail in which a computer that is connected to the application unit also serves as a Message Transfer Agent (MTA);
Figure 6C illustrates an alternative way of communicating using electronic mail in which an application unit includes a message transfer agent for exchanging electronic mail;
Figure 6D illustrates an alternative way of communicating using electronic mail in which a mail server acts as a POP3 server to receive mail for an appliance/device and as an Simple Mail Transfer Protocol (SMTP) server to send mail for the appliance/device;
Figure 7 illustrates an alternative manner of sending messages across the Internet;
Figure 8 illustrates an exemplary computer which may be connected to an appliance/device and used to communicate electronic mail messages;
Figure 9 illustrates an overall system configuration related to the present invention;

ForcePoint LLC
EX-1009
Page140

Figure 10A illustrates a general software architecture of a message sending module;
Figure 10B illustrates a general software architecture of a message receiving module;
Figure 11 illustrates a general architecture of a message sending module;
Figure 12 illustrates a general architecture of a message receiving module;
Figure 13A is a flowchart illustrating a process implemented by the device information module shown in Figure 11;
Figure 13B illustrates a class structure of the device information module;
Figure 14 is a collaboration diagram for the device information module;
Figure 15A is a flowchart illustrating a process implemented by the device monitor module shown in Figure 11;
Figure 15B illustrates a class structure of the device monitor module;
Figures 16, 17 and 18 are collaboration diagrams for the device monitor module;
Figure 19A is a flowchart illustrating a process implemented by the data transfer module shown in Figure 11;
Figure 19B is a flowchart illustrating a process for sending information according to one embodiment of the present invention;
Figure 19C illustrates a class structure of the data transfer module;
Figures 20A, 21, 22, and 23 are collaboration diagrams for the data transfer module in transferring information to monitoring site;
Figure 20B illustrates an exemplary MIME attachment including configuration information according to one embodiment of the present invention;
Figure 20C illustrates an exemplary MIME attachment including status information according to one embodiment of the present invention; and
Figure 24 illustrates a class diagram of the Open Database Connectivity (ODBC) interface module.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0013] Referring now to the drawings, and more particularly to Figure 1 thereof, there are illustrated (1) various machines and (2) computers for monitoring, diagnosing and controlling the operation of the machines. In Figure 1, there is a first network 16, such as a Local Area Network (LAN) connected to computer workstations 17, 18, 20 and 22. The workstations can be any type of computers including, e.g., IBM Personal Computer compatible devices, Unix-based computers, Linux-based computers or Apple Macintoshes. Also connected to the network 16 are (1) a digital image forming apparatus 24, (2) a facsimile machine 28, and (3) a printer 32. As would be appreciated by one of ordinary skill in the art, two or more of the components of the digital image forming apparatus 24 and the facsimile machine 28 can be combined into a unified "image forming apparatus." The devices 24, 28 and 32 and the workstations 17, 18, 20 and 22 are referred to as machines or monitored devices and other types of devices may be used as the machines or monitored devices, including any of the devices discussed below. In some configurations, one or more workstations may be converted to business office appliances. One example of such a business office appliance is eCabinet from Ricoh, which was demonstrated at Fall Comdex in 1999 at Las Vegas. Also, a facsimile server (not illustrated) may be connected to the network 16 and have a telephone, Integrated Services Digital Network (ISDN), cable or wireless connection. In addition to the digital image forming apparatus 24, facsimile machine 28, and printer 32 being connected to the network 16, these devices may also include conventional telephone and/or ISDN and/or cable and/or wireless connections 26, 30 and 34, respectively. As is explained below, the business office machines, business devices, or business office appliances 24, 28 and 32 communicate with a remote monitoring, diagnosis, and control station, also referred to as a monitoring device, through, for example, the Internet via the network 16 or by a direct telephone, ISDN, wireless, or cable connection.

[0014] In Figure 1, a wide area network (WAN) (e.g., the Internet or its successor) is generally designated by 10. The WAN 10 can be either a private WAN, a public WAN or a hybrid. The WAN 10 includes a plurality of interconnected computers and routers designated by 12A-12I. The manner of communicating over a WAN is known through a series of Request for Comments (RFC) documents available from the Internet Engineering Task Force (IETF) at http://www.ietf.org/rfc.html, including RFC 821 entitled "Simple Mail Transfer Protocol"; RFC 822 entitled "Standard for the Format of ARPA Internet Text Message"; RFC 959 entitled "File Transfer Protocol (FTP)"; RFC 2045 entitled "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"; RFC 1894 entitled "An Extensible Message Format for Delivery Status Notifications"; RFC 1939 entitled "Post Office protocol - Version 3"; and RFC 2298 entitled "An Extensible Message Format for Message Disposition Notifications." The contents of each of these references are incorporated herein by reference.

[0015] Transmission Control Protocol/Internet Protocol (TCP/IP) related communication is described, for example, in the book "TCP/IP Illustrated," Vol. 1, The Protocols, by W.R. Stevens, from Addison-Wesley Publishing Company, 1994, the entire contents of which is incorporated herein by reference. Volumes 1-3 of "Internetworking with TCP/IP" by Comer and Stevens are also incorporated herein by reference in their entirety.

[0016] In Figure 1, a firewall 50A is connected between the WAN 10 and the network 16. A firewall is a device that

ForcePoint LLC
EX-1009
Page141

allows only authorized computers on one side of the firewall to access a network, computers or individual parts on the other side of the firewall. Firewalls are known and commercially available devices and/or software (e.g., SunScreen from Sun Microsystems Inc.). Similarly, firewalls 50B and 50C separate the WAN 10 from a network 52 and a workstation 42, respectively. Additional details on firewalls can be found in "Firewalls and Internet Security" by W. R. Cheswick, and S. M. Bellovin, 1994, AddisonWesley Publishing, and "Building Internet Firewalls" by D. B. Chapman and E. D. Zwicky, 1995, OReilly & Associates, Inc. The entire contents of those two references are incorporated herein by reference.

[0017] The network 52 is a conventional network and includes a plurality of workstations 56, 62, 68 and 74. These workstations may be in different departments (e.g., marketing, manufacturing, design engineering, and customer service departments) within a single company. In addition to the workstations connected via the network 52, there is a workstation 42, which is not directly connected to the network 52. Information in a database stored in a disk 46 may be shared using proper encryption and protocols over the WAN 10 to the workstations connected directly to the network 52. Also, the workstation 42 includes a direct connection to a telephone line and/or an ISDN and/or a cable and/or a wireless network 44, and the database in disk 46 may be accessed through the telephone line, the ISDN, the cable or wirelessly. The cable used by this invention may be implemented using a cable that is typically used to carry television programming, a cable that provides for high-speed communication of digital data typically used with computers or the like, or any other desired type of cable.

[0018] Information of the business office machines, business devices or business office appliances 24, 28 and 32 may be stored in one or more of the databases stored in the disks 46, 54, 58, 64, 70 and 76. Known databases include (1) SQL databases by Microsoft, IBM, Oracle and Sybase (2) other relational databases, and (3) non-relational databases (including object oriented databases from Computer Associates, JYD Software Engineering, and Orient Technologies). Each of the customer service, marketing, manufacturing, and engineering departments may have their own database or may share one or more databases. Each of the disks used to store databases is a non-volatile memory such as a hard disk or optical disk. Alternatively, the databases may be stored in any storage device including solid state and/or semiconductor memory devices. As an example, disk 64 contains the marketing database, disk 58 contains the manufacturing database, disk 70 contains the engineering database and disk 76 contains the customer service database. Alternatively, the disks 54 and 46 store one or more of the databases.

[0019] In addition to the workstations 56, 62, 68, 74 and 42 being connected to the WAN 10, these workstations may also include a connection to a telephone line, ISDN, cable, or wireless network which provides a secure connection to the machine being monitored, diagnosed and/or controlled, and is used during communication. Additionally, if one communication medium is not operating properly, one of the others can be automatically used for communication.

[0020] A feature of the present invention is the use of a "store-and-forward" mode of communication (e.g., Internet electronic mail, also referred to herein as e-mail) or transmission between a machine and a computer for diagnosing and controlling the machine. Alternatively, the message which is transmitted maybe implemented using a mode of communication that makes direct, end-to-end connections (e.g., using a socket connection to the ultimate destination) such as FTP and Hyper Text Transfer Protocol (HTTP).

[0021] Figure 2 illustrates the mechanical layout of the digital image forming apparatus 24 illustrated in Figure 1. In Figure 2, 101 is a fan for the scanner, 102 is a polygonal mirror used with a laser printer, and 103 designates an Fθ lens used to collimate light from a laser (not illustrated). Reference numeral 104 designates a sensor for detecting light from the scanner. Reference numeral 105 designates a lens for focusing light from the scanner onto the sensor 104, and reference numeral 106 designates a quenching lamp used to erase images on the photoconductive drum 132. There is a charging corona unit 107 and a developing roller 108. Reference numeral 109 designates a lamp used to illustrate a document to be scanned and 110, 111, and 112 designate mirrors used to reflect light onto the sensor 104. There is a drum mirror 113 used to reflect light to the photoconductive drum 132 originating from the polygon mirror 102. Reference numeral 114 designates a fan used to cool the charging area of the digital image forming apparatus, and reference numeral 115 designates a first paper feed roller used for feeding paper from the first paper cassette 117, and reference numeral 116 designates a manual feed table. Similarly, reference numeral 118 designates a second paper feed roller for the second cassette 119. Reference numeral 120 designates a relay roller, 121 designates a registration roller, 122 designates an image density sensor, and 123 designates a transfer/separation corona unit. Reference numeral 124 designates a cleaning unit, 125 designates a vacuum fan, 126 designates a transport belt, 127 designates a pressure roller; and 128 designates an exit roller. Reference numeral 129 designates a hot roller used to fix toner onto the paper, 130 designates an exhaust fan and 131 designates the main motor used to drive the digital image forming apparatus.

[0022] Figure 3 is a block diagram illustrating the electronic components of the digital image forming apparatus of Figure 2. The CPU 160 is a microprocessor and acts as the system's controller. Random access memory (RAM) 162 stores dynamically changing information including operating parameters of the digital image forming apparatus. A non-volatile memory (e.g., a read only memory 10 (ROM) 164 or a Flash Memory) stores (1) the program code used to run the digital image forming apparatus and (2) static-state data, describing the copier (e.g., the model number, serial

ForcePoint LLC
EX-1009
Page142

number of the copier, and default parameters).

[0023] There is a multi-port network interface 166 which allows the digital image forming apparatus to communicate with external devices through at least one network. Reference number 168 represents a telephone, ISDN, or cable line, and numeral 170 represents another type of network. Additional details of the multi-port network interface are described with respect to Figure 4. An interface controller 172 is used to connect an operation panel 174 to a system bus 186. The operation panel 174 includes standard input and output devices found on a digital image forming apparatus including a copy button, keys to control the operation of the copier such as number of copies, reduction/enlargement, darkness/lightness, etc. Additionally, a liquid crystal display may be included within the operation panel 174 to display parameters and messages of the digital image forming apparatus to a user.

[0024] A local connection interface 171 is a connection through local ports such as RS232, the parallel printer port, USB, and IEEE 1394. FireWire (IEEE 1394) is described in Wickelgren, I., "The Facts About "FireWire", IEEE Spectrum, April 1997, Vol. 34, Number 4, pp. 19-25, the entire contents of which are incorporated herein by reference. Preferably, a "reliable" communication protocol is used which includes error detection and retransmission.

[0025] A storage interface 176 connects storage devices to the system bus 186. The storage devices include a flash memory 178, which can be substituted by a conventional Electrically Erasable Programmable Read Only Memory (EEPROM), and a disk 182. The disk 182 includes a hard disk, optical disk, and/or a floppy disk drive. There is a connection 180 connected to the storage interface 176 which allows for additional memory devices to be connected to the digital image forming apparatus. The flash memory 178 is used to store semi-static state data which describes parameters of the digital image forming apparatus which infrequently change over the life of the copier. Such parameters include the options and configuration of the digital image forming apparatus. An option interface 184 allows additional hardware such as an external interface to be connected to the digital image forming apparatus. A clock/timer 187 is utilized to keep track of both the time and date and also to measure elapsed time.

[0026] On the left side of Figure 3, the various sections making up the digital image forming device are illustrated. Reference numeral 202 designates a sorter and contains sensors and actuators used to sort the output of the digital image forming device. There is a duplexer 200 which allows a duplex operation to be performed by the digital image forming device and includes conventional sensors and actuators. The digital image forming device includes a large capacity tray unit 198 which allows paper trays holding a large number of sheets to be used with the digital image forming device. The large capacity tray unit 198 includes conventional sensors and actuators.

[0027] A paper feed controller 196 is used to control the operation of feeding paper into and through the digital image forming device. A scanner 194 is used to scan images into the digital image forming device-and includes conventional scanning elements such as a light, mirror, etc. Additionally, scanner sensors are used such as a home position sensor to determine that the scanner is in the home position, and a lamp thermistor is used to ensure proper operation of the scanning lamp. There is a printer/imager 192 which prints the output of the digital image forming device, and includes a conventional laser printing mechanism, a toner sensor, and an image density sensor. The fuser 190 is used to fuse the toner onto the page using a high temperature roller and includes an exit sensor, a thermistor to assure that the fuser 190 is not overheating, and an oil sensor. Additionally, there is an optional unit interface 188 used to connect to optional elements of the digital image forming device such as an automatic document feeder, a different type of sorter/collator, or other elements which can be added to the digital image forming device.

[0028] Figure 4 illustrates details of the multi-port network interface 166. The digital image forming device may communicate to external devices through a token ring interface 220, a cable modem unit 222, which has a high speed connection over cable, a conventional telephone interface 224, which connects to a telephone line 168A, an ISDN interface 226, which connects to an ISDN line 168B, a wireless interface 228, or an ethernet interface 230, which connects to a LAN 170. Other interfaces may include, but are not limited to, a Digital Subscriber Line (DSL) (original DSL, concentric DSL, and asymmetric DSL). A single device which connects to both a Local Area Network and a telephone line is commercially available from Megahertz and is known as the Ethernet-Modem.

[0029] The CPU or other microprocessor or circuitry executes a monitoring process to monitor the state of each of the sensors of the digital image forming device, and a sequencing process is used to execute the instructions of the code used to control and operate the digital image forming device. Additionally, there is (1) a central system control process executed to control the overall operation of the digital image forming device, and (2) a communication process used to assure reliable communication to external devices connected to the digital image forming device. The system control process monitors and controls data storage in a static state memory (e.g., the ROM 164 of Figure 3), a semi-static memory (e.g., the flash memory 178 or disk 182), or the dynamic state memory (e.g., a volatile or non-volatile memory (e.g., the RAM 162 or the flash memory 178 or disk 182). Additionally, the static state memory may be a device other than the ROM 164 such as a non-volatile memory including either of the flash memory 178 or disk 182.

[0030] The above details have been described with respect to a digital image forming device, but the present invention is equally applicable to other business office machines or devices such as an analog copier, a facsimile machine, a scanner, a printer, a facsimile server, or other business office machines, a business office appliance, or other appliances

ForcePoint LLC
EX-1009
Page143

(e.g., a microwave oven, VCR, digital camera, cellular phone, palm top computer). Additionally, the present invention includes other types of devices which operate using store-and-forward or direct connection-based communication. Such devices include metering systems (including gas, water, or electricity metering systems), vending machines, or any mechanical device (e.g., automobiles) that needs to be monitored during operation or remote diagnosis. In addition to monitoring special purpose machines and computers, the invention can be used to monitor, control, and diagnose a general purpose computer that would be the monitored and/or controlled device.

[0031] Figure 5 illustrates an alternative system diagram of the present invention in which different devices and subsystems are connected to the WAN 10. However, there is no requirement to have each of these devices or subsystems as part of the invention. Each component or subsystem illustrated in Figure 5 is individually part of the invention. Further, the elements illustrated in Figure 1 may be connected to the WAN 10 which is illustrated in Figure 5. In Figure 5, there is illustrated a firewall 50-1 connected to an intranet 260-1. A service machine 254 connected to the intranet 260-1 includes therein, or has connected thereto, data 256 that may be stored in a database format. The data 256 includes history, performance, malfunction, and any other information such as statistical information of the operation or failure or set-up the monitored devices, or configuration information such as which components or optional equipment is included with the monitored devices. The service machine 254 may be implemented as the device or computer which requests the monitored devices to transmit data, or which requests that remote control and/or diagnostic tests be performed on the monitored devices. The service machine 254 may be implemented as any type of device, and is preferably implemented using a computerized device such as a general purpose computer.

[0032] Another sub-system of Figure 5 includes a firewall 50-2, an intranet 260-2, and a printer 262 connected thereto. In this sub-system, the functions of sending and receiving electronic messages by the printer 262 (and similarly by a copier 286) are performed by (1) circuitry, (2) a microprocessor, or (3) any other type of hardware contained within or mounted to the printer 262 (i.e., without using a separate general purpose computer).

[0033] An alternate type of sub-system includes the use of an Internet Service Provider 264 which may be any type of Internet Service Provider (ISP), including known commercial companies such as America Online, Earthlink, and Niftyserve. In this sub-system, a computer 266 is connected to the ISP 264 through a digital or analog modem (e.g., a telephone line modem, a cable modem, modems which use any type of wires such as modems used over an Integrated Services Digital Network (ISDN) line or an Asymmetric Digital Subscriber Line (ADSL), modems which use frame relay communication, wireless modems such as a radio frequency modem, a fiber optic modem, or a device which uses infrared light waves). Further, a business office device 268 is connected to the computer 266. As an alternative to the business office device 268 (or any other device illustrated in Figure 5), a different type of machine may be monitored or controlled such as a digital copier, any type of appliance, security system, or utility meter, such as an electrical, water, or gas utility meter, or any other device discussed herein.

[0034] Also illustrated in Figure 5 is a firewall 50-3 connected to a network 274. The network 274 may be implemented as any type of computer network, (e.g., an ethernet or token ring network). Networking software which may be used to control the network includes any desired networking software including software commercially available from Novell or Microsoft. The network 274 may be implemented as an intranet, if desired. A computer 272 connected to the network 274 may be used to obtain information from a business office device 278 and generate reports such as reports showing problems that occurred in various machines connected to the network, and a monthly usage report of the devices connected to the network 274. In this embodiment, a computer 276 is connected between the business office device 278 and the network 274. This computer receives communications from the network and forwards the appropriate commands or data, or any other information, to the business office device 278. Communication between the business office device 278 and the computer 276 may be accomplished using wire-based or wireless methods including, but not limited to, radio frequency connections, electrical connections and light connections (e.g., an infrared connection, or a fiber optics connection). Similarly, each of the various networks and intranets illustrated in Figure 5 may be established using any desired manner including through the establishment of wireless networks such as radio frequency networks. The wireless communication described herein may be established using spread spectrum techniques including techniques which use a spreading code and frequency hopping techniques such as the frequency hopping wireless technique which is disclosed in the Bluetooth Specification LOA (available at the World Wide Web site www.bluetooth.com), which is incorporated herein by reference.

[0035] Another sub-system illustrated in Figure 5 includes a firewall 50-4, an intranet 260-4, a computer 282 connected thereto, a business office appliance 285 and a copier 286. The computer 282 may be used to generate reports and request diagnostic or control procedures. These diagnostic and control procedures may be performed with respect to the business office appliance 285 and the copier 286 or any of the other devices illustrated in or used with Figure 5. While Figure 5 illustrates a plurality of firewalls, the firewalls are preferable, but optional equipment, and therefore, the invention may be operated without the use of firewalls, if desired.

[0036] Figure 6A illustrates a device/appliance 300 connected to a typical e-mail exchange system which includes components 302, 304,306,308, 310, 312, 314, 316, and 318, which may be implemented in a conventional manner, and are adapted from Figure 28.1 of Stevens, above. A computer interface 302 interfaces with any of the application

ForcePoint LLC
EX-1009
Page144

units or devices/appliances 300 described herein. While Figure 6A illustrates that the device/appliance 300 is the sender, the sending and receiving functions may be reversed in Figure 6A. Furthermore, if desired, the user may not be needed to interface with the device/appliance 300 at all. The computer interface 302 then interacts with a mail agent 304. Popular mail agents for Unix include MH, Berkeley Mail, Elm, and Mush. Mail agents for the Windows family of operating systems include Microsoft Outlook and Microsoft Outlook Express. At the request of the computer interface 302, the mail agent 304 creates e-mail messages to be sent and, if desired, places these messages to be sent in a queue 306. The mail to be sent is forwarded to a Message Transfer Agent (MTA) 308. A common MTA for Unix systems is Sendmail. Typically, the message transfer agents 308 and 312 exchange communications using a TCP/IP connection 310. Notably, the communication between the message transfer agents 308 and 312 may occur over any size network (e.g., WAN or LAN). Further, the message transfer agents 308 and 312 may use any communication protocol. In one embodiment of the present invention, elements 302 and 304 of Figure 6A reside in the library to monitor the usage of the application unit.

[0037] From the message transfer agent 312, e-mail messages are stored in user mailboxes 314 which are transferred to the mail agent 316 and ultimately transmitted to the user at a terminal 318 which functions as a receiving terminal.

[0038] This "store-and-forward" process relieves the sending mail agent 304 from having to wait until a direct connection is established with the mail recipient. Because of network delays, the communication could require a substantial amount of time during which the application would be unresponsive. Such an unresponsiveness is generally unacceptable to users of the application unit. By using, e-mail as the store-and-forward process, retransmission attempts after failures occur automatically for a fixed period of time (e.g., three days). In an alternate embodiment, the application can avoid waiting by passing communicating requests to one or more separate threads. Those threads can then control communication with the receiving terminal 318 while the application begins responding to the user interface again. In yet another embodiment in which a user wishes to have communication completed before continuing, direct communication with the receiving terminal is used. Such direct communication can utilize any protocol not blocked by a firewall between the sending and receiving terminals. Examples of such protocols include File Transfer Protocol (FTP) and Hyper Text Transfer Protocol (HTTP).

[0039] Public WANs, such as the Internet, are generally not considered to be secure. Therefore, if it is desired to keep messages confidential, messages transmitted over the public WANs (and multi-company private WANs) can be encrypted. Encryption mechanisms are known and commercially available which may be used with the present invention. For example, a C++ library function, crypt(), is available from Sun Microsystems for use with the Unix operating system. Other encryption and decryption software packages are known and commercially available and may also be used with this invention. One such package is PGP Virtual Private Network (VPN) available from Network Associates. Other VPN software is available from Microsoft Corporation.

[0040] As an alternative to the general structure of Figure 6A, a single computer may be used which functions as the computer interface 302, the mail agent 304, the mail queue 306 and the message transfer agent 308. As illustrated in Figure 6B, the device/appliance 300 is connected to a computer 301 which includes the message transfer agent 308.

[0041] A further alternative structure is shown in Figure 6C in which the message transfer agent 308 is formed as part of the device/appliance 300. Further, the message transfer agent 308 is connected to the message transfer agent 312 by a TCP/IP connection 310. In the embodiment of Figure 6C, the device/appliance 300 is directly connected to the TCP/IP connection 310 with an e-mail capability. One use of the embodiment of Figure 6C includes using a facsimile machine with an e-mail capability (e.g., as defined in RFC 2305 (a simple mode of facsimile using Internet mail)) as the device/appliance 300.

[0042] Figure 6D illustrates a system in which a device/appliance 300 does not by itself have the capability to directly receive e-mail, but has a connection 310 to a mail server/POP3 server including a message transfer agent 308 and a mail box 314 so that the device/appliance 300 uses the POP3 protocol to retrieve received mail from the mail server.

[0043] Figure 7 illustrates an alternative implementation of transferring mail and is adapted from Figure 28.3 of Stevens referenced previously. Figure 7 illustrates an electronic mail system having a relay system at each end. The arrangement of Figure 7 allows one system at an organization to act as a mail hub. In Figure 7, there are four MTAs connected between the two mail agents 304 and 316. These MTAs include local MTA 322A, relay MTA 328A, relay MTA 328B, and local MTA 322D. The most common protocol used for mail messages is SMTP (Simple Mail Transfer Protocol) which may be used with this invention, although any desired mail protocol may be utilized. In Figure 7, 320 designates a sending host which includes the computer interface 302, the mail agent 304, and the local MTA 322A. The device/appliance 300 is connected to, or alternatively included within, the sending host 320. As another case, the device/appliance 300 and host 320 can be in one machine where the host capability is built into the device/appliance 300. Other local MTAs 322B, 322C, 322E and 322E may also be included. Mail to be transmitted and received may be queued in a queue of mail 306B of the relay MTA 328A. The messages are transferred across the TCP/IP connection 310 (e.g., an Internet connection or a connection across any other type of network).

[0044] The transmitted messages are received by the relay MTA 328B and if desired, stored in a queue of mail 306C.

ForcePoint LLC
EX-1009
Page145

The mail is then forwarded to the local MTA 322D of a receiving host 342. The mail may be placed in one or more of the user mailboxes 314 and subsequently forwarded to the mail agent 316, and finally forwarded to the user at a terminal 318. If desired, the mail may be directly forwarded to the terminal without user interaction.

[0045] The various computers used in the present invention, including the computers 266 and 276 of Figure 5, may be implemented as illustrated in Figure 8. Further, any other computer used in this invention may be implemented in a similar manner to the computer illustrated in Figure 8, if desired, including the service machine 254, computer 272, and computer 282 of Figure 5. However, not every element illustrated in Figure 8 is required in each of those computers.

[0046] In Figure 8, the computer 360 includes a CPU 362 which may be implemented as any type of processor including commercially available microprocessors from companies such as Intel, AMD, Motorola, Hitachi and NEC. There is a working memory such as a RAM 364, and a wireless interface 366 which communicates with a wireless device 368. The communication between the interface 366 and device 368 may use any wireless medium (e.g., radio waves or light waves). The radio waves may be implemented using a spread spectrum technique such as Code Division Multiple Access (CDMA) communication or using a frequency hopping technique such as that disclosed in the Bluetooth specification.

[0047] There is a ROM 370 and a flash memory 371, although any other type of non-volatile memory (e.g., Erasable Programable ROM, or an EEPROM) may be used in addition to or in place of the flash memory 371. An input controller 372 has connected thereto a keyboard 374 and a mouse 376. There is a serial interface 378 connected to a serial device 380. Additionally, a parallel interface 382 is connected to a parallel device 384, a universal serial bus (USB) interface 386 is connected to a universal serial bus device 388, and also there is an IEEE 1394 device 400, commonly referred to as a fire wire device, connected to an IEEE 1394 interface 398. The various elements of the computer 360 are connected by a system bus 390. A disk controller 396 is connected to a floppy disk drive 394 and a hard disk drive 392. A communication controller 400 allows the computer 360 to communicate with other computers (e.g., by sending e-mail messages) over a telephone line 402 or a network 404. An I/O (Input/Output) controller 408 is connected to a printer 410 and a hard disk 412, for example using a SCSI (Small Computer System Interface) bus. There is also a display controller 416 connected to a CRT (Cathode Ray Tube) 414, although any other type of display may be used including a liquid crystal display, a light emitting diode display, a plasma display, etc.

[0048] Figure 9 illustrates an application of the present invention. Devices 901, 903, 905 and 907 that are connected to the Intranet 910 are the devices to be monitored locally by a remote monitoring workstation 911 with its database 913. Alternatively, the remote monitoring workstation 911 can function to send the device status information to the central monitoring workstation 945 by polling the information from the monitored devices 901, 903, 905, and 907 and by sending the information through the firewall 917. The remote monitoring workstation 911, therefore, can function either as a monitoring device or as a communication and administrative device between the monitored devices and monitoring device. In Figure 9, the remote monitoring workstation 911 uses the Simple Network Management Protocol (SNMP) defined by IETF to communicate with the attached devices. SNMP is described in "Managing Internetworks with SNMP, third edition" by Mark A. Miller, P.E., M & T Book, 1999. The entire contents of this reference are incorporated herein by reference. If some of the devices to be monitored do not support SNMP, the remote monitoring workstation 911 can use a different method to obtain the necessary information. After obtaining the necessary information, the remote monitoring workstation 911 uses the Simple Mail Transfer Protocol (SMTP) Server 915 to send out the necessary information to the central monitoring workstation 945 through the Mail Server 943 that supports the Post Office Protocol Version 3 (POP3) (IETF Networking Group Request For Comments [RFC]: 1939). The remote monitoring workstation 911 uses SMTP (SMTP is defined in IETF RFC 821) and possibly Multipurpose Internet Mail Extensions (MIME) to send e-mails. The remote monitoring workstation 911 generates the mail message that is at and above the Application Layer of the TCP/IP model or the ISO seven-layer model, as shown later. Alternatively, the remote monitoring workstation 911 may include an SMTP processor to send out the necessary information using e-mail.

[0049] The LAN 920 and intranet 930 send similar information to the central monitoring workstation 945. When the e-mails that contain the monitoring information of devices arrive at the firewall 941 of the intranet 950, the mail is routed to the Mail Server 943 with POP3. The central monitoring workstation 945 periodically accesses the Mail Server 943 to obtain the arrived e-mail, parse the mail and its content via POP3 and stores the necessary information in the database 947. The database 949 contains the additional information of the monitored device characteristics and history. The computers 951 and 953 perform the analysis of obtained data to take the necessary actions. Alternatively, the central monitoring workstation 945 may contain a mail receiving capability, and the firewall may route the e-mail directly to the central monitoring workstation 945.

[0050] Figures 10A and 10B illustrate an overall software architecture of the system shown in Figure 9 according to one embodiment of the present invention. Figure 10A illustrates the architecture of the software used by the networks that send the e-mails with the information on the monitored devices in Figure 9 according to one embodiment of the present invention. The Sender Service 1001 module is the system resident software that sets up the destination for the monitored information to be sent, initiates the sending of the configuration and contact information to the destination, and periodically monitors and sends the information to the destination by using the three functions defined in 1000 (i.

ForcePoint LLC
EX-1009
Page146

e., setDestination, obtainAndUpdateStatus, and sendConfig) to trigger the send module, Monitor_Send DLL 1003. The Monitor_Send DLL 1003 module uses two other modules, the Database 1005 module to store the device information and device-related information along with the monitored information that is stored until it is sent out, and the SNMP++ DLL 1007 module that is used to obtain the information from the devices.

[0051] Figure 10B illustrates the architecture of the software used by the receiving side (e.g., intranet 950) in Figure 9 according to one embodiment of the present invention. The Receiver Service 1011 module is the system resident software that sets up access to the mail server where the monitored information is to be sent, and periodically obtains the monitored information from the mail server through the two functions defined in 1010 (i.e., setupPOP3Server, and getMailAndUpdateDatabase) to trigger the Receive_Store DLL 1013 module. The Receive_Store DLL 1013 module uses two other modules, the Database 1017 module to store device information and device-related information along with the monitored information and the POP3 1015 module to retrieve information from the mail server.

[0052] Figure 11 illustrates the general architecture of the Monitor_Send DLL 1003 module according to one embodiment of the present invention. This part of the system is responsible for monitoring the status of the devices and for sending e-mails containing status and configuration information of the monitored devices. The Interface 1101 module allows any application to use the Monitor_Send DLL 1003 module. For example, the Sender Service 1001 module in Figure 10A accesses the Monitor_Send DLL 1003 module through the Interface 1101 module. The Device Information 1105 module is responsible for obtaining configuration information from the monitored devices and initiating the sending of the configuration information. The Device Monitor 1103 module is responsible for obtaining status information from the monitored devices and initiating the sending of the status information. The Data Transfer 1107 module is responsible for providing a method through which the status and configuration information is sent. The ODBC Interface 1109 module provides a method to access and store information in a database. Each of the components of the Monitor_Send DLL 1003 module provides interface functions that allow them to perform its tasks. For example, the functions of the Data Transfer 1107 module are provided through four interface functions, setDestination, startSend, dataSend, and endSend.

[0053] Figure 12 illustrates a general architecture of the Receive_Store DLL 1013 module according to one embodiment of the present invention. This part of the system is responsible for retrieving the information that was sent to it by the Monitor_Send DLL 1003 module and storing the information in the database. The Interface 1101 module allows any application to use the Receive_Store DLL 1013 module. For example, the Receiver Service 1011 module in Figure 10B accesses the Receive_Store DLL 1013 module through the Interface 1101 module. The Receive Manager 1203 module is responsible for obtaining the configuration information and status information of the monitored devices from the POP3 server and storing that information in the database. The Data Retriever 1205 module is responsible for retrieving the data from the POP3 server. The POP3 Processor 1207 module is responsible for accessing the information sent to it by the Monitor_Send DLL 1003 module. The Parser 1211 module is responsible for parsing the information obtained from the POP3 server. The ODBC Interface 1109 module is responsible for storing the information sent to it in a database. Each of the components of the Receive_Store DLL 1013 module provides interface functions that allow them to perform its tasks.

[0054] Figure 13A is a flowchart providing an overview of the functions performed by the Device Information 1105 module in the context of the system diagram of Figure 9. This process focuses on the sending of configuration information of the monitored devices from the remote monitoring workstation 911 to the central monitoring workstation 945, and not the sending of status information, which is described below in the context of the Device Monitor 1103 module. Configuration information for the monitored devices maintained by the central monitor may be either originally sent, or updated, through the functions performed by the Device Information 1105 module, as will be understood in light of the description provided herein.

[0055] As shown in Figure 13A, the process begins with step S1301 where the database 913 is queried by the remote monitoring workstation 911 to obtain configuration information and IP address information corresponding to the devices being monitored by that particular remote monitoring workstation 911. The process then proceeds to step S1302 where, using the IP address obtained from the database 913, the remote monitoring workstation 911 queries the individual monitored devices using SNMP commands to obtain a device-unique identifier (e.g., a MAC address) for each of the devices being monitored. The process then proceeds to step S1303 where the remote monitoring workstation 911 stores the device-unique identifier in the database. The process then proceeds to step S1304 where the configuration information, including the IP address obtained from the database 913 and the device-unique identifier obtained through SNMP commands, are formatted into a common map structure. The process then proceeds to step S1305 where the configuration information including the device-unique identifier is sent to the central monitoring workstation 945 via an e-mail message through the SMTP server 915. Once the information has been sent, the process ends.

[0056] Figure 13B is a class diagram illustrating one embodiment of the Device Information 1105 module of Figure 11 according to the present invention. The Device Information 1105 module is responsible for triggering the Data Transfer 1107 module to start the sending of configuration information, obtaining the device configuration information from the database 913 via the ODBC Interface 1109 module, obtaining a device-unique identifier (e.g., a MAC address)

ForcePoint LLC
EX-1009
Page147

from the monitored SNMP devices and updating the device configuration information in the database 913 to include the device-unique identifier, formatting the device configuration information into a map structure, sending the map structure to the Data Transfer 1107 module, and completing the sending of the configuration information via the Data Transfer 1107 module.

[0057] The database 913 is not initially populated with a device-unique identifier for the monitored devices. The Device Information 1105 module is responsible for obtaining this information from the monitored devices based on information that is originally stored in the database (e.g,. IP address information), via SNMP commands. The device-unique identifier, obtained directly from the devices, is then populated by the Device Information 1105 module into the database 913.

[0058] The map structure used in storing the information to be sent from the remote monitoring workstation 911 to the central monitoring workstation 945 is a standard structure for storing key/value data. Each entry in the map includes a key indicating what the data represents, and a data field containing the value of the data. In one embodiment of the present invention, the key of the map is a string or a number associated with a particular data field, and the data field is a string value. Map structures are included with the standard C++ language, and similar structures, sometimes called a dictionary structure, are included with other standard languages. An example of a populated map structure is shown below as Table 1:

Table 1:

Example Map Structure Including Configuration Information	
Key	**Value (Data)**
"Manufacturer" (or 100)	"Xerox"
"Model" (or 101)	"DocuPrint N4025"
"SerialNumber" (or 102)	"PF4-027955"
"MACAddress" (or 103)	"00 00 AA 79 07 76"
"IPAddress" (or 104)	"172.30.4.53"
"CompanyName" (or 105)	"Ricoh Corporation"
"Street" (or 106)	"1996 Lundy Ave"
"City" (or 107)	"San Jose"
"State" (or 108)	"CA"
"ZipCode" (or 109)	"95131"
"Location" (or 110)	"Lab"
"ContactPerson" (or 111)	"John Smith"
"PhoneNumber" (or 112)	"4085551212"

[0059] The Device Information 1105 module contains two classes, CDeviceInformation 1301 and CIP_MACmap 1303. The CDeviceInformation 1301 class is responsible for obtaining the configuration information from the database 913, and initiating the sending of the information through e-mail from the remote monitoring workstation 911 to the central monitoring workstation 945. The CDeviceInformation 1301 class interacts with the database 913 via the ODBC Interface 1109 module to obtain the configuration information, and uses the Data Transfer 1107 module to transmit the configuration information to the central monitoring workstation 945.

[0060] The CIP_MACmap 1303 class makes use of the CSnmpResource 1305 class to obtain a physical address (e.g., a MAC address) from the monitored SNMP devices. The MAC address is used to uniquely identify the monitored devices within the database 947 maintained by, for example, the central monitoring workstation 945. While an IP address, for example, may uniquely identify a monitored device among the devices connected to a particular network monitored by the remote monitoring workstation 911, that address may not be unique among all of the networks being monitored by the central monitoring workstation 945. It is for this reason that, in this example, a MAC address is used to provide a globally unique identification for a particular device that can be relied on by the central monitoring workstation 945.

[0061] If other device-unique identification is available, the class structure shown in Figure 13B can be modified to accommodate that unique identification.

[0062] Figure 14 is a collaboration diagram illustrating the interaction among the classes of the Device Information

ForcePoint LLC
EX-1009
Page148

1105 module shown in Figure 13B to obtain and send configuration information of a monitored device from the remote monitoring workstation 911 to the central monitoring workstation 945. As shown in Figure 14, the process is initiated by a call to the sendConfig() method of the CDeviceInformation 1403 class by the Interface 1101. In response, the CDeviceInformation 1403 class calls the startSend() method of the CDataTransfer 1405 class to initiate a communication link for sending of the e-mail message that will contain the configuration information. The CDeviceInformation 1403 class then calls the getDeviceInformation() method of the CSendODBCInterface 1411 class to obtain the configuration information, including the IP address, of the monitored device from the database. The CDeviceInformation 1403 class then calls the getMACforIp() method of the CIP_MACmap 1407 class to obtain a physical address (e.g., the MAC address) for the monitored devices based on the IP address that was obtained from the database. In turn, the CIP_MACmap 1407 class calls the setIPAddressOfAgent() and getOctetStringValueForOID() methods of the CSnmpResource 1409 class to query the monitored device based on its IP address to receive its physical address through the appropriate SNMP functions. Next, the CDeviceInformation 1403 class calls the setDeviceInformation() method of the CSendODBCInterface 1411 class to store the configuration information in the database.

[0063] The CDeviceInformation 1403 class then calls the dataSend() method of the CDataTransfer 1405 class to send the configuration information, along with the physical address information, to the central monitoring workstation 945. Finally, the CDeviceInformation 1403 class calls the endSend() method of the CDataTransfer 1405 class to complete the sending of the configuration information.

[0064] Figure 15A is a flowchart providing an overview of the functions performed by the Device Monitor 1103 module in the context of the system diagram of Figure 9. This process focuses on the collection, storing, and sending of information of the monitored devices from the remote monitoring workstation 911 to the central monitoring workstation 945 as an e-mail message via the SMTP server 915.

[0065] As shown in Figure 15A, the process begins with step S1501 where it is determined whether information is to be sent to the central monitoring workstation 945. In one embodiment of the present invention, some information is sent from the remote monitoring workstation 911 to the central monitoring workstation 945 at a different frequency (e.g., less frequently) than a frequency that the monitored devices are polled for status. If it is determined that the collected information is not to be sent to the central monitoring workstation 945 (i.e., "NO" at step S1501), the process proceeds to step S1502 where the monitored devices are polled for a first type of information only.

[0066] The first type of information may include, for example, certain status information that may change states more frequently than information is reported to the central monitoring workstation. A second type of information may include a different class of status information, for example, a counter, a level indicator, or a configuration setting of a monitored device. For this second type of information, interim values between reporting periods are not of interest. As would be understood, it is quite possible that, depending on the frequency with which information is sent to the central monitoring workstation 945, status information corresponding to the first type of information, for example, an error condition, could have been corrected between transmissions to the central monitoring workstation 945. For that reason, it is helpful to store the first type of information, so that when information is sent to the central monitoring workstation 945, it can be reported that, in this example, a particular error condition, while not necessarily still present, had occurred since the last time information was sent. Accordingly, when the information, including both the first type and the second type of information, is sent to the central monitoring workstation 945, the first type of information stored in the database 913 is queried from the database 913 and sent along with the most recent information. Then, those values in the database 913 are reset to clear any information that had been stored leading up to the transmission to the central monitoring workstation 945.

[0067] Returning to Figure 15A, once the first type of information has been collected from the network device, the process proceeds to step S1503 where the first type of information is stored in the database 913 by the remote monitoring workstation 911. After the first type of information is stored in the database 913, the process ends.

[0068] If, on the other hand, it is determined that information is to be sent to the central monitoring workstation 945 (i.e., "YES" at step S1501), the process proceeds to step S1504 where the monitored devices are polled for both the first type of information and the second type of information. Once this information is obtained, the process proceeds to step S1505 where the database is queried for the stored first type of information previously collected. The process then proceeds to step S1506 where both the first type and the second type of information just collected, as well as the first type of information retrieved from the database, is formatted into a common map structure. This is the same map structure that was used by the Device Information 1105 module to send the configuration information. The process then proceeds to step S1507 where both the first type and second type of information is sent by the remote monitoring workstation 911 to the central monitoring workstation 945 as an e-mail message via the SMTP server 915. After the status information has been sent by the remote monitoring workstation 911, the process proceeds to step S1508 where, as discussed above, the remote monitoring workstation 911 resets the values corresponding to the first type of information stored in the database 913 to clear any conditions that may have been recorded leading up to the sending of the information. Once the database 913 values arereset, the process ends.

[0069] Figure 15B is a class diagram illustrating one embodiment of the Device Monitor 1103 module of Figure 11

ForcePoint LLC
EX-1009
Page149

according to the present invention. The Device Monitor 1103 module is responsible for logging and maintaining information about the network devices. This Device Monitor 1103 module is also responsible for ensuring that the information is sent to the central monitoring workstation 945. If the information is not to be sent upon being collected, the Device Monitor 1103 module obtains and stores only certain types of information (e.g., occurrence of no toner, door open, jam, etc.) in the database 913. If the information is to be sent upon being collected, the Device Monitor 1103 module obtains other types of information, including, for example, less volatile status information. The Device Monitor 1103 module includes three classes, CDeviceStatusMonitorAndSendManager 1601, CDeviceStatusLogger 1603, and CSnmpResource 1607.

[0070] The CDeviceStatusMonitorAndSendManager 1601 class is responsible for obtaining the information from the monitored devices and sending the information to the central monitoring workstation 945. The CDeviceStatusMonitorAndSendManager 1601 class uses the Data Transfer 1107 module discussed above to send the information to the central monitoring workstation 945.

[0071] The CDeviceStatusLogger 1603 class is responsible for logging and maintaining the information of the monitored devices. The CDeviceStatusLogger 1603 class obtains and stores information of the monitored devices in the database 913 using the ODBC Interface 1109 module discussed above. The CDeviceStatusLogger 1603 class includes the DevicePerStatus structure for storing the first type of information of the monitored devices in the database 913. In one embodiment of the present invention, only this first type of information is stored in the database.

[0072] The CSnmpResource 1607 class is responsible for providing the network management protocol (e.g., SNMP) which provides the capability for collecting the information from the monitored devices. The CSnmpResource 1607 class uses the SNMP++ DLL 1609 to implement the Simple Network Management Protocol to gather the information from the monitored devices.

[0073] Figure 16 is a collaboration diagram illustrating the interaction among the classes of the Device Monitor 1103 module to obtain and store the first type of information from the monitored devices. As discussed above, if the information collected from the monitored devices is not to be sent to the central monitoring workstation 945 upon collection, only this first type of information is collected and stored in the database 913. As shown in Figure 16, the process is initiated by the CDeviceStatusMonitorAndSendManager 1601 class invoking the logDevicePerStatus() method of the CDeviceStatusLogger 1603 class to initiate the collection and storing of the first type of information of the monitored devices. The CDeviceStatusLogger 1603 class then calls the getDevicePerStatus() method of the ODBC Interface 1109 module to obtain the latest information of the monitored devices, including the IP addresses of the devices, from the database 913. Next, the CDeviceStatusLogger 1603 class calls the setIPAddressOfAgent() method of the CSnmpResource 1607 class which, in turn, calls the set_address() method of the SNMP++ DLL 1609 to establish an IP address of a device from which the first type of information is to be collected. Next, the CDeviceStatusLogger 1603 class calls the getOctetStringValueForOID() method of the CSnmpResource 1607 class which, in turn, calls the get() method and the get_value() method of the SNMP++ DLL 1609 to obtain the latest information of the monitored devices via SNMP using the IP address of the device. Once the information has been returned, the CDeviceStatusLogger 1603 class calls the setDevicePerStatus() method of the ODBC Interface 1109 module to store the information of the monitored devices in the database 913 using the DevicePerStatus 1505 structure.

[0074] Figure 17 is a collaboration diagram illustrating the interaction among the classes of the Device Monitor 1103 module to obtain both a first type and a second type of information from the monitored devices and to reset the values corresponding to the first type of information stored in the database 913 for each monitored device. As discussed above, if the information collected from the monitored devices is to be sent to the central monitoring workstation 945 upon collection, both the first type of information and the second type of information is collected. As shown in Figure 17, the process is initiated by the CDeviceStatusMonitorAndSendManager 1601 class invoking the getNextDeviceStatus() method of the CDeviceStatusLogger 1603 class to initiate the collection of the information (both the first type, and the second type of information) of the monitored devices. Steps 2-8 in collecting both types of information are the same as steps 2-8 described above (i.e., the calls to getDevicePerStatus(), setIPAddressOfAgent(), set_Address(), getOctetStringValueForOID(), get(), get_value(), and setDevicePerStatus()) in the context of Figure 16 for collecting only the first type of information. However, the call to the setDevicePerStatus() method of the ODBC Interface 1109 module in this case (i.e., step 8) is used to reset the values corresponding to the first type of information stored in the database.

[0075] After resetting the values in the database, the CDeviceStatusLogger 1603 class calls the getStringValueForOID() method of the CSnmpResource 1607 class which, in turn, calls the get() and get_printable_value() methods of the SNMP++ DLL 1609 module to obtain the second type of information from the monitored devices via SNMP commands.

[0076] Figure 18 is a collaboration diagram illustrating the interaction among the classes of the Device Monitor 1103 module to send both the first type and second type of information of the monitored devices to the central monitoring workstation 945. As shown in Figure 18, the process is initiated by the CDeviceStatusMonitorAndSendManager 1601 class invoking the getNextDeviceStatus() method of the CDeviceStatusLogger 1603 class to obtain the information of

ForcePoint LLC
EX-1009
Page150

the monitored devices as discussed above in the context of Figure 17. Next, the CDeviceStatusMonitorAndSendManager 1601 class calls the startSend() and dataSend() methods of the Data Transfer 1107 module to initiate the sending of the information to the central monitoring workstation 945. Then, the CDeviceStatusMonitorAndSendManager 1601 class iteratively calls the getNextDeviceStatus() method of the CDeviceStatusLogger 1603 class to obtain information from a monitored device, followed by a call to the dataSend() method of the CDataTransfer 1405 class, shown in Figure 19C, of the Data Transfer 1107 module to send the information for a particular monitored device to the central monitoring workstation 945. Once information has been sent for all of the monitored devices, the CDeviceStatusMonitorAndSendManager 1601 class calls the endSend() method of the CDataTransfer 1405 class, shown in Figure 19C, of the Data Transfer 1107 module to complete the sending of the information.

[0077] Figure 19A is a flowchart providing an overview of the functions performed by the Data Transfer 1107 module in the context of the system diagram of Figure 9. This process focuses on the Data Transfer 1107 module responsible for sending the configuration and status information, and not the collection of the configuration and status information to be sent, as is described above in the context of the Device Information 1105 module and the Device Monitor 1103 module, respectively.

[0078] As shown in Figure 19A, the process begins with step S1901 where the system registry of the remote monitoring workstation 911 is populated with a source address and a destination address for e-mails transferring status information of the monitored devices. In this example, the source address will be the e-mail address of the remote monitoring workstation 911, and the destination address will be the e-mail address of the central monitoring workstation 945. Once the source and destination addresses have been populated in the system registry of the remote monitoring workstation 911, the transfer of information may begin.

[0079] The process then proceeds to step S1902 where a transfer of information commences. In step S1902, the remote monitoring workstation 911 accesses its system registry to obtain source and destination e-mail address information that will be used to populate header information for an e-mail message originating from the remote monitoring workstation 911 and having a destination of the central monitoring workstation 945.

[0080] Once the source and destination information has been obtained, the process proceeds to step S1903 where a communication link is established between the remote monitor workstation 911 and a Simple Mail Transfer Protocol (SMTP) Server 915. Once the communication link has been established, the process proceeds to step S1904, where the configuration or status information is sent as an e-mail message from the remote monitoring workstation 911 to the SMTP server 915 via the communication link. The SMTP server 915 will route the e-mail message to the appropriate recipient, in this case, the central monitoring workstation 945. In one embodiment of the present invention, the remote monitoring workstation 911 sends the configuration or status information as a Multipurpose Internet Mail Extensions (MIME) attachment to the Internet e-mail message. As discussed above, the configuration or status information, prior to sending it to the central monitoring workstation 945, is maintained in the database 913. Once the configuration or status information has been sent, the process proceeds to step S1905, where the remote monitoring workstation 911 will shut down the communication link between itself and the SMTP Server 915. Once the communication link has been shut down, the process ends.

[0081] Figure 19B is a flowchart describing in further detail the processing performed in sending configuration or status information as an attachment to an e-mail message (e.g., the process performed in step S1904 of Figure 19A) according to one embodiment of the present invention. As shown in Figure 19B, the sending the configuration or status information begins with step S 1910 where the configuration or status information in the map structure is formatted to be sent. The structure of the map is such that either configuration or status information data may be stored in the map. Once the data to be sent from the remote monitoring workstation 911 to the central monitoring workstation 945 has been formatted, the process proceeds to step S1911 where the data is encrypted. The Data Transfer 1107 module is configured to allow for a level of encryption for a particular application to match that application's needs without impacting the interface of the Data Transfer 1107 module. Once the data is encrypted, the process proceeds to step S1912 where the data is encoded. Once the data has been encrypted and encoded, the process proceeds to step S1913 where the data is sent via the communication link described above, for example, as a MIME attachment to an e-mail message. Once the data has been sent, the process ends.

[0082] The transfer of configuration or status information from the remote monitoring workstation 911 to the central monitoring workstation 945 has been described in the context of Figures 19A and 19B as using a store-and-forward protocol. Using a store-and-forward approach, for example, SMTP and POP3, the e-mail message is sent via the SMTP server 915 to a mail server, for example mail server POP3 943, in Figure 9. The mail server POP3 will store the e-mail message until it is retrieved by the intended recipient, which, in the example discussed above, is the central monitoring workstation 945. When the central monitoring workstation 945 connects to the mail server POP3 943, the mail server POP3 will forward all messages it has stored that have the central monitoring workstation 945 as an intended recipient.

[0083] Figure 19C is a class diagram illustrating one embodiment of the Data Transfer 1107 module of Figure 11 according to the present invention. The Data Transfer 1107 module is responsible for formatting the configuration or status information collected from the monitored devices, and for sending that information as an attachment to an e-

ForcePoint LLC
EX-1009
Page151

mail message from a remote monitoring workstation 911 to a central monitoring workstation 945, using, for example, SMTP. In one embodiment of the present invention, the monitoring information is sent as a MIME attachment to an e-mail message. The Data Transfer 1107 module is also responsible for encrypting the data and encoding the encrypted data using, for example, Base64 encoding before sending the data. The Data Transfer 1107 module includes six classes: CDataTransfer 1405, CSendManager 1903, CAbsEncrypter 1905, CNullEncrypter 1907, CBase64Encoder 1909, and CSmtp 1911.

[0084] The CDataTransfer 1405 class provides the interface through which the functionality supported by the Data Transfer 1107 module is accessed. In one embodiment of the present invention, the CDataTransfer 1405 class includes four public methods through which all of the functionality of the Data Transfer 1107 module may be accessed. These methods include a setDestination() method, a startSend() method, a dataSend() method, and an endSend() method. The setDestination() method is used to configure both a source and destination address for an e-mail from a remote monitoring workstation 911 to a central monitoring workstation 945. The startSend() method is used to initiate communications between the remote monitoring workstation 911 and a SMTP server 915. The dataSend() method is used to send the monitoring information as an e-mail message from the remote monitoring workstation 911 to the central monitoring workstation 945 via the SMTP server 915. The dataSend() method supports the sending of either configuration information or status information. The endSend() method is used to shut down the communication link after the configuration or status information has been sent. While the Data Transfer 1107 module includes significantly more capabilities, the complexities of these capabilities are hidden from the public interface.

[0085] Returning to Figure 19C, the CSendManager 1903 class includes classes that implement encrypting, encoding, and the management of a communication link between the remote monitoring workstation 911 and the SMTP server 915. CAbsEncrypter 1905 is an abstract class providing the flexibility to add new encryption methods by adding new derived classes of CAbsEncrypter 1905, such as, for example, CNullEncrypter 1907. This class structure provides the flexibility for an application to implement the desired level of encryption, or to change an encryption method without impacting the interface to the Data Transfer 1107 module.

[0086] The CBase64Encoder 1909 class provides base 64 encoding of the information before the information is sent. The CSmtp 1911 class is responsible for managing the communication link between the remote monitoring workstation 911 and the SMTP server 915. CSmtp 1911 makes use of the CSystemRegistry 1915 class for accessing the system registry to determine a source and destination e-mail address for the e-mail message header to be sent to the SMTP server 915. Furthermore, CSmtp 1911 makes use of the CSocket 1917 class available in the Microsoft foundation classes (MFC) for establishing and taking down the communication link between the remote monitoring workstation 911 and the SMTP server 915.

[0087] Figure 20A is a collaboration diagram illustrating the interaction among the classes of the Data Transfer 1107 module shown in Figure 19C when a remote monitoring workstation 911 initiates communication by establishing a link to the SMTP server 915. In Figure 20A, the user 2001 corresponds to either the Device Monitor 1103 module or the Device Information 1105 module. As shown in Figure 20A, the process is initiated by the user 2001 invoking the startSend() method of the CDataTransfer 1405 class. In calling the startSend() method, the user 2001 indicates which type of information (e.g., configuration information or status information) will be sent.

[0088] Figure 20B illustrates an exemplary MIME attachment including configuration information, as can be determined by the first line of the MIME attachment. Figure 20C, on the other hand, illustrates an exemplary MIME attachment including status information, as is also indicated by the first line of the MIME attachment. As described above, it is the startSend() method that ensures that the first line is appropriately populated. The exemplary MIME attachments shown in Figures 20B and 20C are neither encrypted nor encoded.

[0089] Returning to Figure 20A, once the user 2001 has requested the initiation of communications, the CDataTransfer 1405 class will call the startSend() method of the CSendManager 1903 class. The CSendManager 1903 class manages the establishment of a communication link between the remote monitoring workstation 911 and the SMTP server 915 through interactions with the CSmtp 1913 class, which, in turn, interacts with the CSocket 2013 class.

[0090] In order to use SMTP, the CSendManger 1903 class calls the createSocket() method of the CSmtp 1913 class to create a socket to the SMTP server 915 through which the SMTP commands will be sent. Next, the CSendManager 1903 class calls the connectSocket() method of the CSmtp 1913 class to connect to that socket of the SMTP server 915. In response, the CSmtp 1913 class will call the Connect() and Receive() methods of the CSocket 2013 class to connect to the socket.

[0091] Once the socket has been established and connected to, the CSendManager 1903 class calls the sendHeloConunand() method of the CSmtp 1913 class to send the HELO SMTP command to the SMTP server 915. In response the CSmtp 1913 class will call the Send() method of the CSocket 2013 class to send the command to the socket of the SMTP server 915, and subsequently call the Receive() method of the CSocket 2013 class to receive a response from the socket of the SMTP server 915. Using the same approach, the CSendManager 1903 class will send the MAIL, RCPT, and DATA SMTP commands to the SMTP server 915 by respectively calling the sendMailCommand(), sendRcptCommand(), and sendDataCommand() methods of the CSmtp 1913 class. In response to each of the calls, the

ForcePoint LLC
EX-1009
Page152

CSmtp 1913 class will call the Send() and Receive() methods of the CSocket 2013 class to send the commands to, and receive a response from, the socket of the SMTP server 915, respectively.

[0092] As would be understood by those of ordinary skill in the SMTP art, the HELO SMTP command is used by a client, for example, the remote monitoring workstation 911, to identify itself to the SMTP server 915, the MAIL SMTP command is used to identify the originator of a mail message, the RCPT SMTP command is used to identify the recipient for a mail message, and the DATA SMTP command is used to send the contents of a mail message.

[0093] Next, the CSendManager 1903 class calls the sendMailHeader() method of the CSmtp 1913 class to send the mail header for the e-mail message. The CSmtp 1913 class then calls the Send() method of the CSocket 2013 class to send the header to the socket of the SMTP server 915. At this point, the information to be included in the e-mail message can be sent through the socket of the SMTP server 915. The data corresponding to the appropriate information type of the monitored devices is sent by the CDataTransfer 1405 class calling the sendData() method of the CSendManager 1903 class.

[0094] Figure 21 is a collaboration diagram illustrating the interaction among-the classes of the Data Transfer 1107 module shown in Figure 19C to send either status or configuration data through e-mail in response to the Device Monitor 1103 module or the Device Information 1105 module, respectively. In Figure 21, the user 2001 corresponds to either the Device Monitor 1103 module or the Device Information 1105 module. As shown in Figure 21, the process is initiated by the user 2001 calling the dataSend() method of the CDataTransfer 1405 class. The user 2001 sends the map containing the configuration or status information as a parameter of the dataSend() method. The dataSend() method provides a single interface, through which both the Device Monitor 1103 module and the Device Information 1105 module provide information to be sent to the Data Transfer 1107 module. In response, the CDataTransfer 1405 class calls the sendData() method of the CSendManager 1903 class to send the information to the SMTP server 915. In one embodiment of the present invention, each call to the sendData() method of CSendManager 1903 class sends one key/data value pair stored in the map to the socket (steps 8 and 9 shown in Figure 21 are illustrative of this approach). Prior to sending the data, however, the CSendManager 1903 class calls the encryptData() method of the CNullEncrypter 1907 class (or, as described above, another class derived from the CAbsEncrypter 1905 abstract class) to encrypt the data to be sent.

[0095] Next, the CSendManager 1903 class calls the encodeData() and getEncodedString() methods of the CBase64Encoder 1911 class to encode the encrypted data. To send the encrypted and encoded data, the CSendManager 1903 class calls the sendData() method of the CSmtp 1913 class, which, in turn, calls the Send() method of the CSocket 2013 class.

[0096] Figure 22 is a collaboration diagram illustrating the interaction among the classes of the Data Transfer 1107 module shown in Figure 19C when the sending of the configuration or status information through e-mail has been completed.. In Figure 22, the user 2001 corresponds to either the Device Monitor 1103 module or the Device Information 1105 module. As shown in Figure 22, the process is initiated by the user 2001 calling the endSend() method of the CDataTransfer 1405 class. In response, the CDataTransfer 1405 class calls the sendData() method of the CSendManager 1903 class to send data indicating the end of the data to be sent. While it is not shown in Figure 22, the data sent will be encrypted and encoded following the same approach as that described above in the context of Figure 21. Next, the CDataTransfer 1405 class calls the endSend() method of the CSendManager 1903 class to complete the sending. The CSendManager 1903 class completes the sending of data by first calling the endOfData() and getEncodedString() methods of the CBase64Encoder 1911 class to obtain the last encoded information to be sent. Next, the CSendManager 1903 class calls the sendData() method of the CSmtp 1913 class to send the last encoded encoded string containing data. To send the last encoded string, the CSmtp 1913 class calls the Send() method of the CSocket 2013 class.

[0097] Next, the CSendManager 1903 class calls the sendEndOfMail() method of the CSmtp 1913 class to send the end of the mail data. In turn, the CSmtp 1913 class calls the Send() method of the CSocket 2013 class to send the end of the mail data through the socket of the SMTP server 915 followed by a call to the Receive() method of the CSocket 2013 class to obtain a response from the socket. Next, the CSendManager 1903 class calls the sendQuitCommand() method of the CSmtp 1913 class to send the QUIT SMTP command to the socket of the SMTP server 915 to terminate the e-mail session between the remote monitoring workstation 911 and the SMTP server 915. In response, the CSmtp 1913 class calls the Send() and Receive() methods of the CSocket 2013 class to send the QUIT command and obtain a response from the socket.

[0098] Figure 23 is a collaboration diagram illustrating the interaction among the classes of the Data Transfer 1107 module shown in Figure 19C to set up the system registry of the remote monitoring workstation 911 for sending device configuration and status information through e-mail to the central monitoring workstation 945. As shown in Figure 23, the process is initiated by a call to the setDestination() method of the CDataTransfer 1405 class by the Interface 1101. In response, the CDataTransfer 1405 class calls the setDestination() method of the CSendManager 1403 class, which, in turn, calls the setDestination() method of the CSmtp 1913 class. To store the information in the system registry, the CSmtp 1913 class calls the setSMTPServer(), setFromAddr(), and setRcptAdd() methods of the CSystemRegistry

ForcePoint LLC
EX-1009
Page153