

DOCKET NO.: 130839.00921

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Blair NICODEMUS et al.**

Title: **METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING
RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES**

Serial No.: **Not Yet Determined**

Group Art Unit: **Not Yet Determined**

Filed: **Herewith**

Examiner: **Not Yet Determined**

Filed by EFS Web on: **16 August 2012**

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

Dear Sir:

PRELIMINARY AMENDMENT

Prior to examination on the merits, Applicants respectfully request that the application be amended as follows.

Amendment of the Specification begins at page 2.

Remarks begin at page 3.

In the Specification:

Please amend the following paragraphs of the Application at page 1 of the Specification.

Cross-Reference to Related Applications

[001] This application is a continuation application of U.S. Application No. 11/451,950 filed June 13, 2006, which claims the benefit of U.S. Provisional Application No. 60/752,424 filed December 21, 2005, each of which is incorporated herein by reference in its entirety.

[002] This application is related to co-pending U.S. Patent Application No. 11/451,689 ~~{attorney docket number: 1291U004S00}~~ Titled: Methods And Systems For Intelligently Controlling Access to Computing Resources, filed June 13, 2006, now abandoned, on same date herewith, the entirety of which is incorporated herein by reference.

REMARKS

This application is a continuation application of U.S. Patent Application No. 11/451,950 filed June 13, 2006, which claims the benefit of U.S. Provisional Application No. 60/752,424 filed December 21, 2005. Paragraph [001] of the priority claim has been amended. Paragraph [002] has been amended to add the co-pending application serial number. No new matter has been introduced.

CONCLUSION

This Preliminary Amendment is being filed contemporaneously with the continuation application, which are being filed contemporaneously with a Petition for an Extension of Time in the parent application, U.S. Patent Application No. 11/451,950, extending the deadline for response to August 17, 2012.

Applicants respectfully submit this continuation application for examination. The Examiner is invited to contact Applicants' undersigned representative if there are any questions regarding the captioned application.

Respectfully submitted,

by: /Michael A. Patane, Reg. #42982/
Michael A. Patane
Registration No. 42,982

Dated: 16 August 2012
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Streets
Philadelphia, PA 19103-2799
(215) 981 - 4997 (Telephone)
(610) 640 - 7835 (Facsimile)

Electronic Acknowledgement Receipt

EFS ID:	13512441
Application Number:	13587505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair NICODEMUS
Customer Number:	86308
Filer:	Michael Patane/Samantha Rizzo
Filer Authorized By:	Michael Patane
Attorney Docket Number:	130839.00921
Receipt Date:	16-AUG-2012
Filing Date:	
Time Stamp:	16:36:01
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	Application Data Sheet	921 ADS.pdf	/6898 61cccc9f90cda57a9a881a0d1c4f04e0603c	no	5

Warnings:

Information:

This is not an USPTO supplied ADS fillable form					
2		921CONApplication.pdf	<div>9/990/0</div> <div>125a916a615a65a7a2a114a68939c75a13cc7b</div>	yes	118
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	109	
	Claims		110	117	
	Abstract		118	118	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	921FIGS.pdf	<div>738106</div> <div>02d9db1238b48578a6784872c9d48c3d987286</div>	no	7
Warnings:					
Information:					
4	Oath or Declaration filed	CONDec.pdf	<div>804020</div> <div>a73d39d7249a722cd95cc5b7bd99a678c74ed1</div>	no	6
Warnings:					
Information:					
5	Preliminary Amendment	921PrelimAmend.pdf	<div>77723</div> <div>c9737ac941128539c38679e3d17a2b26ba6874c255</div>	no	3
Warnings:					
Information:					
Total Files Size (in bytes):			11495817		

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.

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	
		Application Number	
Title of Invention	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		
<p>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.</p> <p>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.</p>			

Secrecy Order 37 CFR 5.2

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

Applicant Information:

Applicant 1					
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	
				☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Blair		NICODEMUS		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	North Wales	State/Province	PA	Country of Residence	US
Citizenship under 37 CFR 1.41(b)		US			
Mailing Address of Applicant:					
Address 1		143 Polo Drive			
Address 2					
City	North Wales	State/Province	PA		
Postal Code	19454	Country	US		
Applicant 2					
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	
				☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Billy	Edison	STEPHENS		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	West Chester	State/Province	PA	Country of Residence	US
Citizenship under 37 CFR 1.41(b)		US			
Mailing Address of Applicant:					
Address 1		1104 Highgrove Drive			
Address 2					
City	West Chester	State/Province	PA		
Postal Code	19380	Country	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
☐	An Address is being provided for the correspondence information of this application.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	
		Application Number	
Title of Invention	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		
Customer Number	86308		
Email Address	bwdocket@pepperlaw.com	<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		
Attorney Docket Number		Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	

Publication Information:

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

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	86308		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.			
Prior Application Status	Pending	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	11/451950	2006-06-13
Prior Application Status	Expired	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11/451950	non provisional of	60/752424	2005-12-21

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	
		Application Number	
Title of Invention	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		

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

Foreign Priority Information:

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

Remove			
Application Number	Country ¹	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			☐ Yes ☒ No

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

Assignee Information:

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

Assignee 1

If the Assignee is an Organization check here. ☒

Organization Name FIBERLINK COMMUNICATIONS CORPORATION

Mailing Address Information:

Address 1	1787 Sentry Park West, Building Eighteen		
Address 2	Suite 200		
City	Blue Bell	State/Province	PA
Country ¹	US	Postal Code	19422
Phone Number		Fax Number	
Email Address			

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

Signature:

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

Signature	/Michael A. Patane, Reg. No. 42982/		Date (YYYY-MM-DD)	2012-08-16
First Name	Michael	Last Name	Patane	Registration Number
				42982

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	
		Application Number	
Title of Invention	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		

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.

Methods and Systems for Controlling Access to Computing Resources Based on Known
Security Vulnerabilities

Cross-Reference to Related Applications

[001] This application claims the benefit of U.S. Provisional Application No. 60/752,424 filed December 21, 2005, incorporated herein in its entirety.

[002] This application is related to co-pending U.S. Patent Application No. [attorney docket number: 1291U004US00] Titled: Methods And Systems For Intelligently Controlling Access to Computing Resources, filed on same date herewith, the entirety of which is incorporated herein by reference.

Field Of The Invention

[003] The present invention relates generally to electronic computer security, and more specifically to methods and systems for controlling access to computing resources based on known computing security vulnerabilities.

Background Of The Invention

[004] Electronic communication is becoming the industry standard for business communications. Increasingly, office files, design documents, employee work products, company information, and most other important business information is being created and stored electronically on desktop computers, laptop computers, handheld computing devices (collectively 'personal computing device' or 'computing device') and company networks. At work, employees access such networks, along with their associated corporate computing resources from their local computing device, on a daily basis in order to perform their jobs. Away from work, employees similarly access such networks and resources, typically through remote connections. Numerous types of electronic connections are ubiquitous in the industry and well known to the reader, for example: dial – up connections, wireless connections, high-speed connections of various types, virtual private network connections, and others.

[005] Security of such electronic networks has become a recognized, challenging and growing problem. Inappropriate and/or unauthorized access to such electronic

networks, and the computing resources accessible there through, raises the risk of theft, destruction and/or unauthorized modification of valuable data, information and intellectual property. While local, on – site, security can be easily controlled through physical constraints, remote electronic access to such networks and computing resources, typically referred to as endpoint access control, is a more challenging problem.

[006] Endpoint access controls have followed an incremental, evolutionary path. Prior to the storage of sensitive data and the recognition of the security issues associated therewith, there were no endpoint access controls. However, security issues such as data theft, unauthorized access, fraud, etc., and the resulting concerns, created an industry - wide demand for security solutions.

[007] The first generation of endpoint access control included operating system services that controlled user access to one or more system resources, such as applications, data files, configuration settings, etc. Users were permitted or denied access to these resources based on a variety of factors, such as their login ID (which was authenticated using a secret) and a secured profile of policy settings identifying permissions and/or restrictions. These permissions were generally static in that they were not context sensitive in any other dimension than the user ID. There was no consideration of environmental factors. This static nature of security services embedded into the operating system remains relatively unchanged in many environments, to the present day.

[008] In the next step in the evolutionary path of endpoint security control, a series of point solutions were created that address point security concerns by providing point access control capabilities. Examples of these point solutions include: personal firewalls that restrict inbound and/or outbound access to specified applications, ports, addresses and/or communication protocols; antivirus agents, anti-spyware agents and application white-list management agents that monitor, detect and/or restrict access to specific system resources such as memory, registry keys, etc.; software update agents that automatically update an application if it is not a specified version; data encryption agents that encrypt specific files, the complete contents of specific folders, etc.; and physical access control agents that restrict access to floppy drives, USB drives, CD-ROM drives,

etc. These security agents are one-dimensional in that they look at a single aspect of the endpoint's security posture and make decisions on that basis. There is no integration of data across these security agents - all of these security solutions operate autonomously and completely independent of each other, with little or no communications between them or awareness of the state of other applications running on the endpoint. As with operating system security services, these point solutions are also static. The business logic and configurations of these point solutions are not context sensitive. They typically apply the same rules regardless of the user ID, user location, time of day, presence or absence of other security applications on the endpoint, configuration and state of other security or management applications on the endpoint, etc. While providing relatively stable and secure access control, such static endpoint controls remain inflexible and not adaptable to user and business needs. They are very much in use today in many environments.

[009] In the most recent evolutionary step, context awareness has been introduced into the field of endpoint security control. Functional examples of context awareness capabilities on the market today include: if a named application is not running or is not of a specified minimum version, access to network connectivity or certain applications will be restricted or blocked altogether; if a user is in location X (as determined by an assigned IP address, reachability of a network host, or some other method of automated location determination), the user is permitted outbound access using application X and Y to network servers on subnet Z, however if the user is in location Y (alternatively an unknown location), the user is permitted outbound access using application X and W to network servers on subnet V. In each of these examples, access to a resource (in the first case an application, in the second case the network and communications protocols) is context sensitive in the sense that the access privilege is conditional on the current state of the endpoint (in the first case a certain application running, in the second case the current location). However these solutions are limited in that they are only able to assess a limited set of inputs and affect a narrow set of access privileges. Additionally, once an access privilege has been granted, the decision is rarely revisited over the life of the user's connection or access session, i.e. they could come out of compliance subsequent to granting of access and will still retain access.

[0010] Today's access control solutions still lack significant functions and capabilities. As one example, they lack the ability to form context-based access control decisions using as decision inputs state information provided by point solutions that are not context aware. Further lacking is the ability to collect endpoint state information from multiple point solutions, collect endpoint state information from the environment itself (e.g. information obtained from the operating system), and integrate the collected information to form a higher-level holistic and intelligent view of the overall endpoint state.

[0011] Today's solutions further fail to provide extensibility of the endpoint state information integration function so as to enable the collection and integration of endpoint state information from a wide range of existing and future point solutions, applications and the endpoint environment itself. They lack the ability to define and enforce more granular access control permissions and restrictions, including the extensibility of this granular access control function to future access control objectives.

[0012] Today's endpoint securities solutions do not provide the ability to define conditional, parameter-based business logic with flexible compliance models. They lack the ability to define via configuration settings parameter values for different users and user groups, and further lack the ability to optionally and selectively notify an end user when access control restrictions are being enforced on their endpoint.

[0013] Further desirable, and lacking, are useful, functional, management reports as well as dynamic, functional and user-friendly access control capabilities.

[0014] It will thus be seen that today's endpoint security control systems lack many functionalities and capabilities of importance both to hands-on users and their employers.

Summary Of The Invention

[0015] There are provided herein methods and systems for flexibly managing corporate security policies, typically to control access to local or remote computing resources.

[0016] In one embodiment of the invention there are provided methods and systems for controlling the operation of a computing system in response to a security vulnerability, one exemplary method comprising: the computing system running software subject to at least one security vulnerability; establishing a policy based on the status of the at least one security vulnerability including at least one rule and an analysis method for determining compliance with the rule; receiving information relating to the status of the at least one security vulnerability of the software program; processing the information relating to the status using the analysis method; determining, based on the processing, the compliance of the at least one security vulnerability in relation to the rule; and controlling, based on the determining, the operation of the computing system.

[0017] In another embodiment of the invention there are provided methods and systems for controlling the access of an endpoint computing system to a host computing system in response to a security vulnerability, an exemplary method comprising: identifying within at least one of the endpoint and host systems a plurality of conditions, each condition having a state; operating on at least one of the host computing system and the endpoint computing system a software program subject to at least one security vulnerability; establishing a policy based on the status of the at least one security vulnerability and the state of each of the plurality of conditions, the policy including at least one rule and an analysis method for determining compliance with the rule; receiving information relating to the status of the at least one known security vulnerability of the software program; receiving information relating to the state of each of the plurality of conditions; processing the information relating to the status of the at least one known security vulnerability and the state of each of the plurality of conditions using the analysis method; determining, based on the processing, the compliance of the at least one security vulnerability and the plurality of conditions with the rule; and controlling, based on the determining, access of the endpoint system to a resource of the host computing system.

[0018] In another embodiment of the invention there are provided methods and systems for generating signals to control the access of an endpoint computing system to a resource in a host computing system, an exemplary method comprising: collecting a state for each of a plurality of conditions in at least one of the endpoint computing system and

the host computing system; collecting a status of a known security vulnerability for a software program operating on at least one of the host computing system and the endpoint computing system; identifying a policy for determining access of the endpoint computing system to the resource, the policy including at least one rule and an analysis method for determining compliance with the rule; processing, using the analysis method, the state of each of the plurality of conditions and the status of the known security vulnerability; determining, based upon the processing, if the conditions and the known security vulnerability are in compliance with the rule; and generating, based upon the determining, a signal usable to control the access of the endpoint computing system to the resource.

[0019] In yet another embodiment of the invention there are provided methods and systems for developing a compliance policy to control the access of an endpoint computing system to a resource in a host computing system, an exemplary method comprising: identifying a plurality of conditions in at least one of the endpoint computing system and the host computing system, each of the plurality of conditions including an associated state, at least one of the plurality of conditions relating to a risk of a known security vulnerability; and developing a policy for determining the access of the endpoint computing system to the resource, the policy including a rule and at least one analysis method for processing the states of the plurality of conditions to determine if the plurality of conditions are in compliance with the rule.

Brief Description Of The Drawing Figures

[0020] These and other objects, features and advantages of the present invention will become apparent from a consideration of the following Detailed Description Of The Invention in conjunction with the drawing Figures, in which:

[0021] Figure 1 is a block diagram showing features of a security compliance system in accordance with one embodiment of the present invention;

[0022] Figure 2 is a flow chart showing a process for managing security compliance in accordance with an embodiment of the invention;

[0023] Figure 3, is a functional block diagram showing the interaction of agents, managers, monitors and compliance engine in a security compliance system;

[0024] Figure 4 is a flow chart showing the flow of information between agents, managers, monitors, and the policy management system;

[0025] Figure 5 is a block diagram showing an alternate embodiment of the invention wherein various components of the policy management system are incorporated with in the other computing systems;

[0026] Figure 6 is a flow chart showing a process for integrating known security risks into a compliance system; and

[0027] Figure 7 is a flow chart showing the operation of the analysis engine to analyze agent data and develop a compliance policy.

Detailed Description Of The Invention

[0028] As used here in, examples and illustrations, as well as descriptive terminology such as “exemplary” and “illustrative” and variants thereof, are descriptive and non limiting.

[0029] For purposes of describing the present invention, the following specification is arranged topically, in accordance with the following topics:

- Overview
- Description Of The System
- Establishing Agents And Managers
- Establishing Rules And Policies
- Administrator Policy Configuration
- Integration With Vulnerability Scoring Systems
- Analyzing Agent – Collected Condition Data
- EndPoint Compliance Assessment Algorithms
 - Matrix Analysis Algorithm
 - Business Rules -Based Analytical Model For Policy Enforcement

- Boolean Table - Based Analytic Model For Policy Enforcement
- Scoring – Based Analytical Model For Policy Enforcement
- Individual Agent Score Threshold Analysis And Enforcement
- Composite Agent Scoring, Threshold Analysis And Enforcement
- Complementary Individual And Composite Agent Scoring, Threshold Analysis And Enforcement
- Single Level Versus Multi – Level Agent Scoring, Threshold Analysis And Enforcement
- Continuous Reporting Versus Exception Reporting Threshold Analysis and Enforcement
- Matrix Algebra-Based Analytical Model for Policy Enforcement
- Context-Sensitive Threshold and Weighting Adjustments to Quantitative Analytical Models for Policy Enforcement
- Statistics-Based Analytical Model for Policy Enforcement
- Data Summary-Based Statistical Analysis Methods
- Mean-Based Analysis Method
- Moving Average-Based Statistical Analysis Method
- Median-Based Statistical Analysis Method
- Mode-Based Statistical Analysis Method
- Geometric Mean-Based Statistical Analysis Method
- Rate-Based Statistical Analysis Method
- Acceleration Rate-Based Statistical Analysis Method
- Variability-Based Statistical Analysis Methods
 - Min-Based, Max-Based and Range-Based Statistical Analysis Method
 - Standard Deviation-Based Statistical Analysis Method
 - Coefficient of Variation-Based Statistical Analysis Method
 - Number of Occurrences-Based Statistical Analysis Method
 - Occurrence Frequency-Based Statistical Analysis Method
 - Cumulative Distribution-Based Statistical Analysis Method
 - Sampling Distribution-Based Statistical Analysis Method
 - Sampling Distribution-Based Statistical Analysis Method

- Linear Regression-Based Analysis Method
 - Filtering Analysis
 - Application of Methods to All Endpoint State Data Elements
 - Application of Methods to Non-Numeric Endpoint State Information
 - Application of Analytical Methods to Composite Endpoint Compliance Assessments
 - Exception Reporting of Analyses Result
 - Non-Exclusivity of Analyses Methods
 - Combining Analyses Methods
- Real Time Adjustment of Sampling Frequency
 - Managing Endpoint and Host Operation
 - Communication of Endpoint State Information, Endpoint Compliance Analysis Results And/Or Compliance Actions to a Remote Computer
 - Implementation Method 1 - Endpoint system Only
 - Implementation Method 2 – Centralized endpoint system policy management
 - Implementation Method 3 – Centralized host system policy management
 - Implementation Method 4 – Centralized analysis engine and compliance analysis of individual systems
 - Implementation Method 5 – Centralized analysis engine and compliance analysis of multiple systems
 - Implementation Method 6 – Policy management system as in-band access control mechanism
 - Data Sharing
 - Remote Administrator Notification and Control

Overview

[0030] The present invention provides new and improved methods and systems for flexibly monitoring, evaluating, and initiating actions to enforce security compliance policies. As will be seen from a consideration of the detailed description of the invention, provided below, benefits and advantages of the present invention include:

- o The collection of a wide range of endpoint state information. The enumeration of

- state policies regarding preferred, required and prohibited states.
- The enumeration of action policies regarding required, permitted and prohibited actions to take when the endpoint is partially or entirely in or out of compliance with state policies.
 - An analysis engine enabling comparing current states, state policies and action policies and reaching decisions on actions to permit, prevent, or automatically initiate.
 - A flexible methodology for assigning numerical values to current state information, state policies and action policies so that a variety of quantitatively-based analysis models can be used to determine security compliance.
 - An enforcement capability that can operate persistently, constantly measuring compliance, with an ability to dynamically adjust access privileges subsequent to an initial granting of privileges.
 - An ability to create and adjust a 'sliding scale' having different levels of overall security risk tolerance or conversely an overall minimum security threshold that allows or prevents access to specific hardware, software and/or computing resources depending on the degree of compliance with level-specific security policies and in particular the specific types of noncompliance that exist at each level.
 - A compliance analysis engine that supports use of a range of different analytical methods and models so that optimum models can be invoked and applied, depending on situational factors.
 - The initiation of and controlled access to a wide range of software and hardware actions.

Description of the System

[0031] As used here, the terms "illustrative," "example," "includes," and variants thereof are exemplary and not exclusive or otherwise limiting.

[0032] With reference now to Figure 1, there is shown there is shown a system 100, including a host system 102, an endpoint system 104, and a policy management system 106. In accordance with the present invention and conventional use, host system 102 comprises a secure, access-controlled processing system where-to remote systems such as endpoint system 104 connect to access data, processing capacity and host-accessible

resources. Policy management system 106 provides rules and policies concerning the connection of remote endpoint systems 104 to host system 102. Host system 102, endpoint system 104, and policy management system 106, are interconnected to communicate through a conventional electronic network 108, such as the Internet.

[0033] Considering in detail host system 102, the system is seen to include, in a conventional manner, a processor and user & communications interface 102A, as well as conventional storage components 102B, operating systems and software (typically contained in storage and operated by the processor) and other conventional components. Further associated with host system 102 are a variety of resources, indicated at 102G, accessible directly or indirectly through the host, including, for example: user data, user applications, physical ports, data storage devices, dial adaptors, network interfaces, and other resources as will be apparent to the reader. Further contained within host 102 are a plurality of conditions 102F. These conditions are monitored by agents 102E, the agents collecting and transmitting information to agent managers 102D for aggregation by agent monitor 102F. The various conditions, as well as the agent functions, are described in detail herein below. Host 102 may comprise, for example, a processing system of the type typically owned, managed and/or operated by a business to support the operation of its employees. It may comprise a server, enterprise system, personal computer, laptop, personal digital assistant, mobile communications device such as a 'smart' telephone, or any other type of remotely accessible system. In a conventional manner, host system 102 may include conventional security features for controlling access to the data and resources thereon.

[0034] Host system 102 may be consolidated at a single location or comprise a plurality of systems dispersed over multiple locations.

[0035] Continuing with reference to Figure 1, endpoint system 104 comprises any processing system capable of interconnecting with host system 102, for example: a laptop computer, personal computer, server system, enterprise system, personal digital assistant, cellular telephone, 'smart' telephone or other personal device, or any other processing system capable of remotely accessing host system 102 for the purpose of accessing the

resources available there on. Endpoint system 104 is seen to include, in a conventional manner, a processor and user & communications interface 104A, as well as conventional storage components 104B, operating systems and software (typically contained in storage and operated by the processor) and other conventional components. Further contained within host 104 are a plurality of conditions 104F. These conditions are monitored by agents 104E, the agents collecting and transmitting information to agent managers 104D for aggregation by agent monitor 104F. The various conditions, as well as the agent functions, are described in detail herein below.

[0036] Considering now the details of policy management system 106, in the illustrated embodiment, the system comprises a conventional processing system, for example a server computer, enterprise computer, personal computer or a notebook computer. Accordingly, the system is seen to include, in a conventional manner, a processor and user & communications interface 106A, as well as conventional storage components 106B, operating systems and software (typically contained in storage and operated by the processor) and other conventional components. In accordance with the present invention, policy management system 106 is seen to include a compliance analysis engine 106C as well as various policy information stored within storage system 106B. As will be seen from the description below, compliance analysis engine 106C, typically comprising software in data store 106B running on hardware 106A, functions to receive system condition information and process that condition information in accordance with the security policies, such as are stored within data storage 106B, in order to generate security rules. Analysis engine 106C can comprise a portion of the capacity of processor 106A and/or one or more dedicated and/or shared separate processor(s).

[0037] In accordance with a feature of the present invention, the policy data stored within data store 106B can contain multiple sets of policy data for use by different endpoint systems 104, for use by different host systems 102 and for use by the policy management system 106 itself.

[0038] In various embodiments as described in further detail below, the functions incorporated and described with respect to policy management system 106 may be contained i) within endpoint system 104, ii) within host system 102, iii) as a stand-alone network device otherwise connected to network 108, and/or iv) distributed in various combinations of the foregoing. See, for example, Figure 5 wherein a compliance analysis engine 106C is shown in each of endpoint systems 104 (engine 106C') and host system 102 (engine 106C''). It will be understood that the various other features of policy management system 106 may be performed by the existing components of the endpoint and host systems, or otherwise duplicated, replicated, or omitted within those systems as required to perform the appropriate functions as described herein. Further, as used herein, references to the policy management system includes where appropriate only those components and functions necessary to perform the described functions.

[0039] In other embodiments of the invention, host system 102 is used to control access to a network, for example a private network. In one such embodiment, host 102 comprises a gateway or other type of access control system to a network such as a private network. In another such embodiment, host 102 functions to make compliance and access assessments in accordance with the present invention, and forwards the results of such assessments to another access controller. In such instances, the present invention is used to control access by an endpoint such as endpoint system 104, to a network, limiting or permitting endpoint system 104 to access specific network resources based on its current level of compliance.

[0040] As described herein, the various subsystems, agents, processes and managers can be implemented using hardware components, software components and/or combinations thereof.

[0041] With reference now to Figure 2, there is shown a process 200 in accordance with the present invention for controlling the access of a user such as endpoint system to a computing resource. As noted above, the present invention may be used to control access between different systems such as an endpoint system and a host system, or within a system, such as to particular resources available within the system.

Establishing Agents & Managers

[0042] As used here in, and generally in accordance with the accepted definition in the art, “agents” operate to determine the status of particular conditions in a system, as described herein the host system 102 and endpoint system 104. It will be understood by the reader that the invention is equally applicable to controlling access to resources within a single system as to between systems. For purposes of explanation, the invention will be described with respect to controlling the access of endpoint system 104 to host system 102. However, as described above, the invention is equally applicable to controlling access within host system 102 and/or endpoint system 104, as well as other computing systems.

[0043] Again, as is generally in accordance with the accepted definitions in the art, an “agent manager” operates to control the function of as well as to aggregate data collected by the various agents. An “agent monitor” functions to aggregate the data collected by various agent managers. The various agents, managers and monitors can be implemented in hardware, software, and/or combinations thereof.

[0044] When used to describe the operation of an agent, the terms “state,” “condition” and variants thereof are used synonymously to describe the status of the agent.

[0045] Considering first the selection of conditions to monitor within endpoint 104 (step 202), there are many different data sources and data elements that can be examined to assess the state of the endpoint, form compliance assessments, and ultimately make policy-based access control decisions regarding local and remote computing resources.

[0046] Individual configuration data elements such as antivirus heuristics scanning status, and state data elements such as ‘is antivirus currently operating’, can be obtained by establishing an interface to an agent specifically designed to collect and report that piece of information. Such configuration states and data elements are indicated in the drawing Figure 1 as conditions 104F. The agents 104E can comprise a component of the endpoint system or an external service provided by third party software. The endpoint system includes one or more agent managers 104D. These agent managers collect state

information from individual agents 104E or the general computing environment, including the operating system version, registry settings, and others as will now be apparent to the reader. An agent monitor 104C functions to collect and process information from the various agent managers 104D, in the manner described below.

[0047] A given inspection agent may provide a granular or broad means to indirectly assess configuration state and data elements and may provide numerous pieces of state configuration and state information to the endpoint's agent managers 104D. For example the response to a query regarding the state of a configuration setting might simply be true or false, whereas the response to a query regarding what viruses are currently being monitored for could be an enumerated list of thousands of virus names.

[0048] Agents running on endpoint 104 and performing related or similar functions can generally be grouped into categories. For example, an antivirus client/agent, an anti-spyware agent, a content filtering agent and an applications white-list agent can be grouped into a 'security agent' category.

[0049] It will be understood by the reader that the universe of monitorable conditions, sources of state information, will expand and evolve over time. For example, new operating system services may come available, new categories of security applications may emerge, security point solutions may become integrated, transport technologies will continue to evolve, transport hardware will evolve, features of security point solutions will evolve, etc. Therefore the present invention contemplates the addition, modification, or removal of agent components as needed over time. Furthermore, different customer needs will warrant monitoring or conversely not warrant monitoring of selected conditions. The present invention is extensible to be able to take advantage of new sources of information as they become commercially available or as customers request support for new or existing products. The agents, managers and policies are also desirably flexible since, depending on the presence or absence of operating system facilities, third party applications, etc. not all condition information may be available simultaneously. Therefore endpoint 104 is configured so as to be able to

add, modify, or remove agents on a per user basis and to further customize or adapt a given configuration of the endpoint's software components over time.

[0050] Illustrative conditions 104F that are available and may be used for assessing endpoint state information are as follows. Note that not all of these conditions will be needed at any one point in time, i.e. when different system events occur, different pieces of endpoint state information become relevant. It will be understood that different items of interest may be monitored at different times, and different users will have different items they are interested in monitoring.

[0051] User state information includes:

- User ID, User group(s) membership (e.g. reseller, customer, business unit, division, department, etc.),
- User role(s)/position (e.g. sales, executive, clerical worker, mobile professional, system administrator, etc.),
- User workgroup, and
- User security group.

[0052] Authentication state information includes:

- Authentication method (e.g. no authentication, reusable password, one time password, biometrics, smart card, etc.),
- Authentication source (E.g. local to the machine or to a remote authentication database across a network),
- Authentication success/failure result, Password strength, Age of password, and Number of successive login failures.

[0053] Endpoint hardware Information includes:

- Endpoint hardware owner (public kiosk, user-owned, corporate asset, etc.)
- Endpoint hostname
- Hardware configuration and state, such as:
 - CPU type
 - Total system memory
 - Free memory

- Etc.
- BIOS:
 - Vendor
 - Version
 - Individual settings
- Drive mappings
- Supported pointing devices
- Enabled and active pointing devices
- Current power source
- Battery charge level
- System temperature

[0054] Endpoint Operating System Information includes:

- Base OS version
- Installed service packs
- Installed patches
- State of OS configuration settings (enabled/disabled options, services settings, option settings, etc.)
- Currently active OS services
- Default language
- Installed language packs

[0055] Operating System Services Information includes:

- Intra-application and Internet-application copy/paste service (e.g. Microsoft Windows Clipboard)

[0056] Network Services Information includes:

- DNS:
 - Current primary and secondary DNS servers
 - Size of DNS cache
 - Number of DNS queries

- DNS queries serviced by local DNS cache
- ICMP:
 - ICMP messages transmitted
 - ICMP messages received
- ARP:
 - Contents of ARP cache
 - Number of ARP requests
 - Number of RARP requests
- Network protocols enabled
- IP settings:
 - Current TTL setting for outbound IP packets
 - IP address
 - Default gateway
 - Subnet mask
- UDP/TCP
 - Window size
- HTTP:
 - HTTP requests sent
 - HTTP request transmission rate
 - Number of requests to a given host
 - Number of requests to a given domain

[0057] Number of requests to a given IP address or address rangeFile System

Information includes:

- Read/write status of a named file
- Access privileges to a named file
- Access privileges to a named folder or directory.
- File being deleted
- File being created
- File being opened
- File being overwritten

[0058] Application Information includes:

- Installed application information
 - Vendor
 - Version
 - Configuration settings
 - License ID
 - Digital signature
- Running applications
- Running processes
- Current priority level for each running application
- Application being opened
- Application being closed
- Memory consumed by each running application
- Application update history information
- Preferred application priority
- Number of times an application is opened, per hour, per day, per week, per month, etc.
- Transaction response time for specific application transactions
- Number of times a specific application transaction occurs

[0059] Application-Specific Information includes:

- Email:
 - Version in use
 - Max number of emails per minute
 - Number of emails received and in inbox or other mail folders
 - Email arrival rate
 - Email reception rate
 - Email attachment count
 - Email attachment size
 - Number of recipients in emails sent
- Web browser:

- URLs being accessed

[0060] Data Information includes:

- Local data being accessed
- Application accessing the local data
- Remote data store being accessed
- Application accessing the remote data
- Remote data elements be accessed
- User access privileges for data being accessed
- Data being copied or saved to a local external storage device (e.g. USB thumb drive)
- Data being transmitted to, copied to, or saved to a remote location
- Remote location data being transmitted to
- Remote location data being retrieved from
- Specific text strings (including support for wildcards and logical AND/OR/ELSE/NOT combinations) contained in a file, in a document, in an email, in a communications message, etc.

[0061] Data Backup Information includes:

- Backup program information
 - Vendor
 - Version
- Backup configuration settings:
 - Specific data to be backed up (e.g. files, folders, modified documents, tables, records, etc.)
 - Backup type (e.g. incremental, whole)
 - Backup destination
- Amount or volume of data to be backed up
- Date of last backup
- Date of next backup

- Backup agent state (e.g. active, idle)

[0062] Antivirus Agent Information includes:

- Antivirus agent information
 - Vendor
 - Version
 - Signature files version
- Antivirus-specific configuration settings, (e.g. scan whole system, specific folders, specific files, run scan at startup, run scan every X days, signatures update frequency, etc.)
- Amount or volume of data to be scanned
- Date of last update
- Antivirus scanning state (e.g. active, idle)

[0063] Personal Firewall Agent Information includes:

- Personal firewall agent information
 - Vendor
 - Version
- Personal firewall-specific configuration settings (e.g. user notify, silently discard, event logging, event log uploads, blocking enabled/disabled, etc.)
- Permitted/Restricted outbound applications, protocols and/or destinations
- Permitted/Restricted inbound applications, protocols and/or destinations
- Date of last software update
- Date of last profile update
- Personal firewall state (e.g. actively blocking, blocking disabled, etc.)

[0064] VPN Client Information includes:

- VPN client program information
 - Vendor
 - Version

- VPN client-specific configuration settings (e.g. default profile, split tunneling, authentication method, etc.)
- Date of last software update
- Date of last profile update
- VPN tunnel state (e.g. connecting, connected, disconnecting, disconnected)

[0065] Anti-Spyware Agent Information includes:

- Anti-spyware agent information
 - Vendor
 - Version
 - Signature files version
- Anti-spyware-specific configuration settings, (e.g. scan, whole system, specific folders, specific files, run scan at startup, run scan every X days, signatures update frequency, etc.)
- Date of last update
- Anti-spyware agent scanning state, (e.g. active, idle)

[0066] Data Encryption Agent Information includes:

- Data encryption agent information
 - Vendor
 - Version
- Data encryption-specific configuration settings
 - Method of user authentication
 - Specific data to be encrypted (e.g. files, folders, modified documents, tables, records, etc.)
 - Encryption type (e.g. AES, digital certificate, TPM chip, etc.)
- Data encryption agent state, (e.g. active, idle)

[0067] Content Filtering Agent Information includes:

- Content filtering agent information
 - Vendor

- Software version
 - Blocked sites file version
- Content filtering agent-specific configuration settings
 - Method of filtering (e.g. local list, proxy server)
 - Specific sites or site categories to be filtered
 - Event logging
 - Log upload
- Content filtering agent state, (e.g. active, idle)
- Date of last software update
- Date of last filter list update
- Local HTTP/HTTPS proxy settings for remote HTTP/HTTPS proxy server

[0068] Asset Management Agent Information includes:

- Asset management agent information
 - Vendor
 - Software version
 - Asset reporting profile version
- Asset management agent-specific configuration settings
 - Information being recorded
 - Log upload destination server
- Asset management agent state, (e.g. active, idle)
- Date of last software update
- Date of last profile update

[0069] Location Information includes:

- Geographic location
- Physical location on the corporate campus
- Location category:
 - Directly connected to corporate network
 - Home
 - Public wireless location

- Hotel
- Approved kiosk
- Public wired broadband location
- Remote and connected to corporate network via a VPN
- Reachability of specific remote hosts or networks

[0070] Time-Based Information includes:

- Local time of day
- Time of day at destination
- Day of week
- Day of month

[0071] Wireless Connection Information includes:

- Permitted SSIDs
- Prohibited SSIDs
- Suspect SSIDs
- Configuration of current wireless connections, e.g.
 - Bluetooth:
 - Current connection details
 - Permitted connections configuration settings
 - Wi-Fi and other IEEE 802.11 wireless data communication link protocols
 - Current connection details, e.g. ad hoc mode, network mode, WEP, WPA, WPA2, 802.1x, key length, etc.
 - Permitted connections configuration settings

[0072] Available Connection Information includes:

- Available network connections
- Specific network devices available (specific adapter or modem in use)
- Network technologies available (Wi-Fi, wired, mobile data, dial, etc.)
- Theoretical bandwidth available

- Cost per minute/cost per megabyte
- Network service provider
- Link encryption options

[0073] Active connection information includes:

- Specific network device in use
- Network technology in use
- Theoretical available bandwidth
- Current bandwidth
- Average bytes/sec output
- Average bytes/sec input
- Cost per minute/cost per megabyte
- Network service provider
- Network printing status
- Link encryption method
- Authentication method
- Network bytes received
- Network bytes transmitted

[0074] Subsequent to identifying the various conditions to be monitored within endpoint system 104 (step 202), the various agents 104E and agent managers 104D and agent monitor(s) 104C are identified and configured for monitoring those various conditions (step 204). For example an agent manager 104D may be configured to query a vendor-specific API exposed by a third party antivirus agent, may be configured to query an operating system service periodically to determine if the endpoint has an active network interface and if so, the IP address of that interface, etc. Multiple managers 104D may be separately configured to monitor multiple agents 104E and multiple monitors 104C configured to aggregate manager data. In summary, agent managers are configured to monitor the conditions of interest such as one or more of those described above.

[0075] Agents can be free standing external software applications, system services provided by the operating system or dedicated, special-purpose monitoring processes that are part of the monitored system itself. Agents can monitor both software activity and hardware activity. A typical method for monitoring hardware information is through the use of hardware device drivers and other similar operating system services. Examples of freestanding agents are antivirus client, personal firewall, anti-spyware, anti-phishing agents, data backup agents, etc. Agent monitor 104C can comprise software, hardware and/or a combination thereof, and is functional to collect or aggregate the input from the various agents, through the agent managers, and communicate that data for processing as described herein.

[0076] With reference now to Figure 3, there is illustrated diagrammatically an exemplary series of agents 104E connected to monitor exemplary endpoint conditions 104F such as those listed above. The agent monitors 104C perform overall endpoint monitoring through the use of individual agent managers 104D, each of which monitors one or more specific agents 104E, the individual agent managers 104D aggregated by an agent management service 104D'. As previously mentioned, different configurations and policies will require the use of different individual agent managers and different specific agents. Further illustrated in Figure 3 is the communication of the agent data to the compliance analysis engine 106C for processing in accordance with the methods described herein below.

Establish Rules & Policies

[0077] With reference now back to Figure 2, subsequent to the identification of the conditions to be monitored and the establishment of the various agents, agent managers and agent monitors as described above, there are next established rules and policies for controlling the access to local resources on the endpoint system 104 or remote host system 102 (step 206).

[0078] The policies established to control access to host system 102 and/or access to local host resources 102G as described above, can specify a number of behavioral options for endpoint system 104. These policies are typically established by the operator of host

system 102 or the administrator of endpoint system 104, and stored in the policies storage section 106B of policy management system 106. Configuration policies specify a number of behavioral options for the client. As described here in, configuration policies include both the configurable behaviors of the compliance analysis engine and the security policies of the systems. Configuration policy behaviors supported by the client include:

[0079] Endpoint inspection management policies, including:

- Enumerated list of endpoint data categories to monitor or not monitor
- Enumerated list of sensors within each category to monitor or not monitor
- Method of monitoring for each sensor (e.g. active polling, or passive receipt of events)
- Frequency of monitoring for each sensor
- Enumerated list of data elements to be sampled with the following parameters identified for each sampled:
 - Whether sampling is to occur a regular basis, or whether it is to be initiated as a result of a system event
 - If sampling is to be initiated in response to a system event:
 - The event (e.g. an application being launched, a network connection being established, a user opening a file, a system login event, an application login event, an antivirus agent compliance violation, etc.)
 - If applicable, a threshold value and type (e.g. 5 times a minute when antivirus compliance score is below 75%, email transmission rates above 5 per minute, etc.)
 - Number of samples to collect for a compliance evaluation cycle
 - Sampling interval (if applicable)
 - Acceleration window interval (if applicable)
 - Whether sampling and results reporting method should utilize a successive stop/start windowing method or a sliding window method (e.g. for moving average-type calculations).
- Enumerated list of data elements to be sampled on a regular or threshold basis,

and the corresponding sampling interval

- Enumerated list of policies and thresholds for which the sampling frequency must be adjusted when a threshold is reached. For each policy one or more of the following parameters must be defined:
 - Threshold value
 - Upper and lower threshold value (for range-based thresholds)
 - Sampling parameters (e.g. count, interval, etc.) when out of range
 - Sampling parameters (e.g. count, interval, etc.) when in range

[0080] Compliance Engine Management, including:

- Enumerated list of analytical model(s) to use for different endpoint data elements
 - Business rules
 - Boolean tables
 - Matrix method 1
 - Matrix method 2
 - Mean method
 - Moving average method
 - Variance method
 - Standard deviation method
 - etc.
- Enumerated list of compliance thresholds for different endpoint data elements:
 - Min value
 - Max value
 - Required range (min and max value)
 - Variance
 - Standard deviation
- Composite scoring inputs:
 - Mandatory inputs
 - Exception based
 - Combined
 - Enumerated list of items that are mandatory inputs into the

- composite score
 - Enumerated list of items that are exception inputs into the composite score
- Composite scoring calculation method:
 - Discrete
 - Time base
 - Sampling interval
 - Number of samples
- Hostname of remote computer management application to which endpoint information should be sent
- Type of information to send to management application, e.g. raw collected data, compliance analysis results, compliance actions scheduled to occur, etc.
- Frequency with which client should query policy management server to look for and retrieve any available policy updates.

[0081] Action Management information including:

- Enumerated list of action categories to enforce or not enforce
- Enumerated list of actions within each action category to enforce or not enforce

[0082] Enumerated State Policies information including:

- Endpoint Hardware Configuration Policies
 - Permitted devices types
 - Required device manufacturer
 - Required device version
 - Minimum free hard drive space
 - Required device serial number
 - Required device asset tag
 - Removable storage device permissions
 - Required operating system version
 - Required operating system patches

- Required operating system configuration settings
- Permitted operating system configuration settings

[0083] Endpoint Data Storage Device Access Policies information including:

- Prerequisites for a named I/O port or storage device to be permitted to be accessed as read only
- Prerequisites for a named I/O port or storage device to be permitted to be accessed as read/write only
- Prerequisites for a named I/O port or storage device to be permitted to be accessed as write only
- Enumerated list of applications permitted to access named I/O ports or storage devices

[0084] Printer Access Storage Policies

- Prerequisites for a named printer to be permitted to be used
- Named applications allowed to access named printers

[0085] Authentication Policies

- Password reset age or date
- Password expiration age or date
- Required user location to allow password reset activation
- Permitted authentication methods for system access
- Permitted users to be logged into this endpoint

[0086] Application Policies

- Permitted applications per named user
- Permitted application versions per named user
- Permitted applications for a specified endpoint hardware configuration
- Permitted transactions per named application per named user

- Prerequisites for a named application to be permitted to run
- Endpoint state conditions that require a named application to be exited immediately.
- Applications to automatically uninstall upon detection
- Applications to automatically uninstall if usage falls below a specified threshold of use (e.g. number of times opened or used per day, per week, per month, etc.)
- Default OS priority level when running
- Preferred OS priority level when average CPU utilization exceeds threshold
- Application priorities when average CPU utilization exceeds threshold
- Application priorities when instant CPU utilization exceeds threshold
- Minimum free memory requirements to be permitted to run a specified application
- Cumulative frequency thresholds for named transactions (e.g. 90% of all new order upload transactions must complete within 5 seconds)
- Enumerated list of applications to back up.
 - Preconditions/prerequisites for initiating backup, e.g.
 - When user is connected to corporate network via a VPN AND
 - User has a wired broadband connection OR
 - User has a Wi-Fi connection
- Required operating system patches to run a specific application
- Required operating system configuration settings to run a specific application
- Required HTTP/HTTPS proxy settings

[0087] Data Access Policies

- Local data permitted to be accessed
- Local data permitted to be modified
- Remote data permitted to be accessed
- Remote data permitted to be modified
- Local files permitted to be deleted
- Remote files permitted to be deleted

- Data permitted to be transmitted to remote locations
- Remote locations data permitted to be transmitted to; Enumerated for each file, folder and/or file type
- Required security posture to have read or read/write privileges to specific data
- Local data permitted to be accessed by authentication method
- Remote data permitted to be accessed by authentication method
- Local data permitted to be modified by authentication method
- Remote data permitted to be modified by authentication method
- Data permitted to be transmitted to remote locations by authentication method
- Data permitted to be transmitted to remote locations by link encryption method

[0088] Data Backup Policies

- Enumerated list of folders and/or files to back up.
 - Preconditions/prerequisites for initiating backup
 - Example:
 - When user is connected to corporate network via a VPN
AND
 - User has a wired broadband connection OR
 - User has a Wi-Fi connection
 - Example:
 - Initiate incremental backup when:
 - When user authentication fails 3 successive times
AND
 - Wired broadband network connection exists OR
Wi-Fi network connection exists
 - Initiate full backup when:
 - When user authentication fails 3 successive times
AND
 - Network connectivity exists over any transport type
 - Initiate full backup when:

- User is connected directly to corporate network OR
User is remotely connected to corporate network via
a VPN AND
 - User authentication fails OR User access privileges
have been revoked
- Maximum number of days, or hours between data backups for incremental
backups
- Maximum number of days, or hours between data backups for full backups
- Data to be backed up in incremental back ups
- Data to be backed up in full back ups
- Data to be backed up when not attached to corporate network
- Data to be backed up when connected via a VPN to corporate network over a
specified transport
- Data to be backed up by specified link encryption method

[0089] Endpoint Location Policies

- Permitted remote locations
- Permitted corporate office locations

[0090] Authentication Policies

- Permitted authentication methods
- Max number of days between password resets
- Max number of authentication failures

[0091] Network Access Policies

- Permitted network addresses and/or address ranges allowed to be accessed by the
user
- Permitted network addresses and/or address ranges allowed to be accessed by a
specific named application
- Required applications to be running in order to enable a specified network adapter

- Required applications to be running in order to enable a specified modem
- Permitted network transports
- Permitted network devices
- Permitted network service providers
- Permitted hotspots
- Permitted dial numbers
- Permitted wired broadband locations
- Permitted link encryption options by transport
- Cost per minute limit
- Cost per megabyte limit
- Permitted authentication methods
- Maximum connection duration by transport
- Maximum bandwidth consumption by transport
- Days of week network connectivity permitted
- Time of day network connectivity permitted
- Permit local application X, Y and Z to have network access
 - When antivirus is running AND
 - When personal firewall is running AND
 - Antivirus vendor is Symantec AND
 - Antivirus version is v5 or greater

[0092] CPU Utilization Policies

- CPU utilization threshold for triggering application prioritization adjustments
- CPU sampling interval
- CPU sampling window
- Sampling method (fixed interval, moving average, combined, etc.)
- Enumerated list of applications to disable if instant CPU utilization threshold exceeded
- Enumerated list of applications to have operating system priority levels forcibly changed if instant CPU utilization threshold exceeded

- Enumerated list of applications to disable if average CPU utilization threshold exceeded
- Enumerated list of applications to have operating system priority levels forcibly changed if average CPU utilization threshold exceeded
- CPU increase rate

[0093] Application-Specific Policies

- Email:
 - Permitted and/or restricted source email addresses or domains
 - Permitted and/or restricted destination email addresses or domains
 - Maximum number of outbound emails per minute
 - Maximum number of inbound emails per minute
 - Permitted recipients when email contains a specific text string (support for wildcards and logical combinations of AND, OR, NOT, ELSE, IF, etc. is supported)
 - Rate of outbound emails
- Web browsers
 - Permitted URLs or domains
 - Restricted URLs or domains
 - Permitted web sites/content
 - Prohibited web sites/content

[0094] File System Policies

- Files to automatically delete upon detection
- Format disk policies, e.g.:
 - When incremental or full backup has occurred within the last e.g. 72 hours
AND
 - User fails authentication 5 successive times
- File protection policies, e.g.:
 - Set data files to read only when e.g.

- When antivirus is not running OR
- When antivirus reports an infected system

[0095] Antivirus Policies

- Permitted vendor(s)
- Permitted product name(s)
- Permitted version(s) for named vendors
- Max permitted antivirus update age
- Required antivirus product
- Required antivirus version
- Required antivirus configuration settings
- Required antivirus runtime status
- Required virus definition files minimum version
- Required frequency of updates to virus definition files
- Enumerated list of virus threats with attack type and severity level identified for each

[0096] Personal Firewall Policies

- Required firewall product
- Required firewall version
- Required firewall configuration settings
- Required firewall runtime status

[0097] Anti-Spyware Policies

- Required anti-spyware agent product
- Required anti-spyware agent version
- Required anti-spyware agent configuration settings
- Required anti-spyware agent runtime status
- Required anti-spyware signature files minimum version

- Required frequency of updates to anti-spyware definition files
- Enumerated list of spyware threats with attack type and severity level identified for each

[0098] Endpoint Patch Management Policies

- Required patch management agent product
- Required patch management agent version
- Required patch management agent configuration settings
- Required patch management agent runtime status
- Required frequency of updates to patch management definition files

[0099] The solution provides the ability to add support for additional policies in the future.

[0100] Wireless Signals Policies

- Minimum signal strength to connect to Wi-Fi transport
- Minimum signal strength to connect to CDMA EV-DO transport
- Minimum signal strength to connect to CDMA 1xRTT transport
- Minimum signal strength to connect to GSM transport
- Minimum signal strength to connect to GPRS transport
- Minimum signal strength to connect to EDGE transport
- Minimum relative signal strength
- Permitted wireless network connectivity modes, e.g. Wi-Fi ad hoc mode, Wi-Fi infrastructure mode, 802.1x authentication required, 802.1x authentication type

[0101] Active Network Connections

- Minimum average bytes out/sec threshold

Administrator Policy Configuration

[0102] The invention includes a graphical user interface application accessible

through 106A that allows an administrator to: view available options for endpoint inspection using centralized policy management system 106, view compliance policies and policy enforcement actions, specify the policies of interest to them, and specify specific values for each policy of interest. All changes made by the administrator are saved to the policy database 106B and made available for all endpoint systems 104 or host systems 102 in the policy group to which those policy settings apply. Alternatively, this functionality could be included in a graphical user interface application on the endpoint system 104 or a graphical user interface application on the host system 102, when users or local administrators of those computing devices are responsible for configuring their own policy settings locally.

[0103] One additional function of the policy management system 106 is the ability to receive and respond to policy update requests from endpoints 104 and hosts 102. The endpoint system 104 and/or host system 102 are configured via a policy setting to periodically query one or more remote policy database(s) 106B residing on the policy management system 106 and retrieve updated information about new policies and updated policy settings. The processor then stores this information in a local data repository.

[0104] Because the number of policy options can be daunting, the policy management system user interface 106A can provide a control that allows an administrator to effectively summarize on a sliding scale, e.g. 1-5, High/Medium/Low, 1-100, etc. their desired security posture, or conversely their security posture noncompliance tolerance. A set of data tables in the policy management database maps each setting on this sliding scale to the enablement and/or disablement of specific policies and policy actions, as well as specific compliance thresholds or scores. This greatly simplifies the administrator's task when establishing and configuring policies. A 'Custom' or comparable user interface control is also made available that allows an administrator to bypass the summary control and directly access the complete set of granular policy settings. The values in the data tables used to map a summary security

level to specific policies and compliance thresholds are of course able to be changed by the database administrator at any time.

Integration With Vulnerability Scoring Systems

[0105] Many computer hardware and software vendors are known to maintain a running list of known security vulnerabilities in their products. See for example vendor Web sites:

- www.microsoft.com/technet/security/alerts/matrix.msp
- www.cisco.com/en/US/products/products_security_advisories_listing.html

As used herein, references to software and software programs to describe a security vulnerability are to be interpreted in their broadest sense, including software such as application programs, operating systems and drivers, combinations of software and hardware and hardware.

[0106] Because each vendor has their own terminology, definitions and subjective view of what constitutes a vulnerability and the degree of risk or exposure a given vulnerability represents (i.e. its severity), there are several industry initiatives to standardize vulnerability definitions and scores. See for example:

- www.kb.cert.org/vuls
- www.first.org/cvss/cvss-guide.html

[0107] Depending on the source, information that may be published about each vulnerability includes information such as descriptive parameters that describe the hardware or software at risk (e.g. Intel-based hardware running Windows XP Service Pack 2), possible system impacts (e.g. memory buffer overflow, unauthorized remote control of the computer, etc), severity type, severity level, sources of more information, date vulnerability was first reported, etc.

[0108] Vendors often use this information to prioritize their responses to vulnerabilities in their products. Responses typically take the form of customer notifications, often accompanied by specific interim remedial actions to take (e.g. disable

a service, shut down a TCP port, etc.) and/or information on currently available patches that can be applied to eliminate the vulnerability.

[0109] When there is no current software available to eliminate the vulnerability, the vendor will normally begin scheduling internal activities to develop a solution to the vulnerability and make the solution available to customers and product users as a 'patch' or 'update'. Once this becomes available, customers may receive notification, and/or find notification information on a vendor's web site.

[0110] Information technology (IT) managers, also referred to herein as administrators, access vulnerability information by either receiving a notification from a vendor or industry group, going to the vendor or industry web site and querying the vulnerability database, or by establishing an electronic communications link with the remote database and electronically receiving vulnerability database updates on a periodic basis. IT managers typically use a combination of industry risk assessment and vendor risk assessment information to prioritize which vulnerabilities and patches to focus on first, and to prioritize remediation activities relative to other routine IT operating activities and other IT projects.

[0111] There is often a significant gap of several days to several months between when a vulnerability is announced by a vendor or an industry watchdog and when the vendor releases a patch or update that addresses that vulnerability. In addition, there is an inevitable gap of days, weeks and possibly even months from the time the patch first becomes available to the time the IT manager becomes aware that the patch is available, retrieves the patch, tests the patch, identifies the end points needing the patch and deploys the patch to all end points and/or hosts needing the patch. This is a very dangerous period of time for endpoint security, during which the system is vulnerable to the identified security risks.

[0112] The interval of time between when a vulnerability is announced and when a vulnerable endpoint is patched commonly referred in the IT industry to as an 'exploit

window', i.e. a window of time in which a security attack that specifically, opportunistically targets that publicized vulnerability can be created and used to probe endpoints to find vulnerable ones that can be attacked. During the exploit window, the endpoints remain exposed to a security attack unless some temporary securing action is taken to protect the endpoint. Attack exposure may be from the local machine only, from a remote machine, or both, depending on the nature of the vulnerability. The attack may utilize only the new exploit or more commonly utilize a combination of exploits to gain control of the system, gain reliable access to the system, take an action on the local system, or have the local system initiate a communications session with a remote computer of the hacker's choosing.

[0113] Combining information sources such as those described above, it is possible using the present invention to create a vulnerability policy directory including but not limited to the following information: Description of hardware and/or software that is vulnerable, descriptive attributes (e.g. whether it is exploitable locally or remotely, whether it impacts data confidentiality, data integrity or computing resource availability, etc.) specific remedial or corrective actions to take to eliminate the vulnerability (e.g. halt an operating service, block a port, block an application, disable a network interface, etc.), and the vulnerability severity level (e.g. high/medium/low, 4 out of 5, 7.5 out of 10, 65%, etc.). The present invention uses this information in accordance with the process shown and described with respect to Figure 6. By using this information to eliminate the vulnerability almost immediately after it the information is publicly available, the present invention is able to provide almost immediate protection for any computing device against vulnerability-specific exploits or security attacks during the period of time between when the security attack is created and used, and when the IT manager or end user has received the software patch from the software vendor and applied that same patch/repair to the computing device. Initially, the security risk information is stored on a data repository, for example within policy management system 106, that is accessible to remote endpoints via communications links, e.g. the Internet (step 602).

[0114] In accordance with this embodiment of the invention, the client software is configured via a policy setting to periodically query one or more remote vulnerability policy database(s) and retrieve updated information about new vulnerabilities and updated information about existing vulnerabilities (step 604). The client then stores this information in a local data repository (step 606).

[0115] The client software is configured via policy settings to examine each vulnerability stored in the local data repository on a periodic basis, or whenever a particular system or policy compliance event warrants (step 608). The client software can subsequently utilize this information in one or more of several different ways to diminish this security risk (step 610), depending on how its policy settings are configured:

- The client can inspect each entry in the vulnerability directory, inspect the endpoint to see if the vulnerability is applicable, and if so, take the corrective action specified. Such capabilities are readily commercially available today.
- The client can inspect each entry in the vulnerability directory, inspect the endpoint to see if the vulnerability is applicable, and if so, examine the severity level and compare that to a policy-defined severity level, and corresponding policy-defined actions to take when a vulnerability with the specified severity level or a higher severity level is found.
 - If the severity level equals or exceeds a specified policy-defined value, then take the corrective action specified.
 - Optionally if enabled via a policy setting, the client can subsequently inspect the endpoint to determine whether the corrective action succeeded or the vulnerable condition still exists.
 - If the corrective action taken does not succeed, consider the endpoint out of compliance and take one or more policy-defined corrective actions, e.g. block access to a file, a folder, an application, network connectivity, establishing a VPN tunnel, provide a notification to the user, etc.

- If the corrective action taken does not succeed, consider the endpoint out of compliance and adjust one or more security compliance scores where applicable. The revised scores when fed into the compliance analysis engine along with other endpoint state data may result in one or more policy-defined corrective actions being taken, e.g. block access to a file, a folder, an application, network connectivity, establishing a VPN tunnel, etc.

[0116] The client can inspect the one or more vulnerability characteristics present in the collective set of information, such as the access vector, (e.g. is the vulnerability exploitable locally or remotely, does it effect confidentiality, integrity or availability, etc.) and compare that to a policy-defined list of characteristics to be on the lookout for, and corresponding policy-defined actions to take when a vulnerability with the specified characteristic is found:

- If the vulnerability characteristic matches a policy-defined value, then take the corrective action specified.
 - Optionally if enabled via a policy setting, the client can subsequently inspect the endpoint to determine whether the corrective action succeeded or the vulnerable condition still exists.
 - If the corrective action taken does not succeed, consider the endpoint out of compliance and take one or more policy-defined corrective actions, e.g. block access to a file, a folder, an application, network connectivity, establishing a VPN tunnel, etc.
 - If the corrective action taken does not succeed, consider the endpoint out of compliance and adjust one or more security compliance scores where applicable. The revised scores when fed into the compliance analysis engine along with other endpoint state data may result in one or more policy-defined corrective actions being taken, e.g. block access to a file, a folder, an application, network connectivity, establishing a VPN tunnel, etc.

Analyzing Agent-Collected Condition Data

[0117] With reference now back to Figure 2, the various condition data described above is collected by the agent managers through the agents (step 208) and then analyzed (step 210). With reference to Figure 4, there is shown in block diagram format the functional aspects 400 of collecting agent data from various exemplary agents 104E, collected through various exemplary agent managers 104D, aggregated by the agent monitoring service 104C for processing by analysis engine 106C, subsequently resulting in one or more actions being taken by various exemplary agents 104E.

[0118] As shown, and described in further detail herein below, the output of analysis engine 106C is a series of actions to take, block and/or permit, the actions communicated back to the agents through the various managers. The aggregated set of actions is passed to the agent management service as a set of instructions. The agent management service parses the instructions, identifies for each instruction the appropriate individual agent manager 104D capable of executing the instruction and passes selected instructions to the appropriate agent manager 104D. The agent manager 104D passes the instructions to the particular agent 104E it relies on to take a particular action. The actions taken by the various agents 104E, for example the control system services, system resources, system hardware, system applications and system data, in endpoint system 104 or host system 102, depend on where the various security functionalities of the invention are installed

[0119] Additionally, the data collected from various exemplary agents 104E and aggregated by the agent monitoring service 104C can be communicated over a data communications network to the policy management system 106 which can also process the collected data using the compliance analysis engine 106C. There are several alternative embodiments. One embodiment (call it embodiment 1) has all data collected at the end point analyzed by a compliance analysis engine residing on the end point, (whether that end point be a laptop or a host system web server). An alternative embodiment (call it embodiment 2) has all data collected at the end point analyzed by a

compliance analysis engine residing on the policy management server. In this latter embodiment, the question is what happens when the policy management server completes the compliance analysis and determines that some policy violations exist and one or more policy compliance actions must be taken. There are several different embodiments possible using the policy management server to perform the compliance analysis function (Call these embodiments 2A, 2B, 2C, etc. Brief embodiment descriptions follow:

Embodiment 2A: Policy management server sends policy action instructions (block this application, permit that application, etc.) back to end point for execution. Note that a best practice would be to digitally sign the instructions sent to the end point using the policy management server's digital certificate. The end point must validate the digital signature before considering the policy action instructions. Embodiment 2B: Policy management server sends instructions (block this end point, permit that end point, limit that end point to only host systems residing on the the 192.168.10.x subnet, etc.) to a network access control device for execution. Normally the access control device will as a result of these instructions add an Access Control List (ACL) entry to its data traffic forwarding table that subsequently effects what destination host systems and communication protocols may be used by the end point when the end point is trying to reach a host server through the network access control device. Embodiment 2C: Policy management server sends instructions (block this end point, permit that end point, limit that end point to only the following applications or application transactions) to a host system for execution. Normally the host system will as a result of these instructions add an Access Control List (ACL) entry to its session management table that subsequently effects what applications or application transactions residing on that host system may be accessed or used by the end point when the end point is requesting services from that host system.

[0120] The policy management server creates a list of permitted host systems, applications, and/or application transactions that the end point is permitted to contact, based on its current degree of compliance. Policy management server then digitally signs the 'permitted actions list' and returns the permitted actions list to the end point. When end point wants to access a host system, the end point presents the digitally signed permitted actions list to the host system. The host then validates the policy manager's digital signature on the signed permitted actions list and then creates an ACL that allows

the end point to access specific resources (e.g. files, folders, types of transactions) on the host system. An alternative and complementary embodiment (Embodiment 2D-2) is that when packets from the end point have to pass through a network access control device residing between the end point and the host system, the end point must authenticate to the network access control device. As part of the authentication process at the network access control device, the end point must present the digitally signed permitted actions list to the network access control device. The network access control device then validates the policy manager's digital signature on the signed permitted actions list and then creates an ACL that allows the end point to access specific host systems (e.g. a single or range of IP addresses) and/or to use specific communication protocols (e.g. FTP, HTTP, SMTP, etc). The policy management system 106, shown connected to the Internet, can be implemented alongside a network access control device, e.g. a router, switch VPN server, etc. or can remotely communicate with the network access control device via a data communications network. In this embodiment, the policy management system 106 is able to communicate access permission and/or access restrictions to the network access control device, restricting what host systems 102 the endpoint system 104 is able to access, restricting what endpoint systems 104 are able to access host systems 102, and/or restricting what remote systems host system 102 is able to access. The policy management system 106, when it has received aggregated information from the agent monitor 104C on endpoint system 104 is also able to send access instructions to host system 102 identifying what permissions or restrictions should be applied to an endpoint system 104 when endpoint system 104 tries to access host system 102 via the network 108. Note that this last embodiment does not require the system 104 to have or be running security-related software such as this invention. Rather, the host system 102 can be protected and/or restrict access with respect to any endpoint 104 that tries to communicate with it.

[0121] Analysis engine 106C (Figure 1) contains one or more analytical methods or models and enables the selection of the optimum model or models for a given set of conditions 104F as determined by the various agents 104E. In accordance with the present invention, a feature and advantage of analysis engine 106C is its support for

multiple models, its extensibility to support future models, and the ability to use multiple different models simultaneously either in parallel or in series while performing compliance analysis of conditions 104F. The analysis engine analytical model compares current condition information 104F, policies regarding those conditions 106B and makes action decisions resulting from those conditions and policies, using one or more analytical models. Analysis engine 106C subsequently initiates actions to permit, deny or control access to local and/or remote computing resources based on additional policies that identified permitted and/or denied actions when a noncompliance condition exists.

[0122] Analytical model selections are based on one or more policy-based configuration settings stored in the policy store 106B. These policies, or rules, may alternatively and/or additionally be locally stored on the endpoint system 104 and/or host system 102, accessed by an endpoint system 104 or a host system 102 from a remote policy management system 106 via a data communications network, or a combination of the two. As with all other policies, the policy setting controlling what analytical models are used and when they are used can be dynamically changed at any time by changing the values of the policy settings in accordance with the processes described above.

[0123] The following sections describe some of the analytical models used by analysis engine 106C. Policy management system 106 is designed to allow analytical models operated by analysis engine 106C to be added in the future, individually upgraded or modified, or removed. Conventional software distribution methods are used to communicate new or modified analytical models and new versions of the analysis engine 106C. In accordance with the present invention, analysis engine 106C is also architected to allow the inputs and/or actions associated with a given policy to be modified or customized as required. Conventional software distribution methods are used to communicate new or modified policies or policy values. Policies incorporating combination rules are also supported through the logical combining of multiple individual rules using conventional logic clauses such as AND, OR, NOT, ELSE, IF, WHEN, UNLESS, etc.

[0124] The analysis engine 106C is the central and primary destination for all

collected or received condition state information collected by the local endpoint system 104. Some or all condition state information to be collected may be requested by the analysis engine on a periodic basis, requested by the analysis engine as a direct result of a detected event, requested by the analysis engine as a direct result of completed analysis of previously received condition state information, sent to the analysis engine by agents and agent managers on a periodic basis, and/or sent from agents or agent managers to the analysis engine as a direct result of a detected event. This holds true for instances of local analysis of condition state information on the endpoint system 104 as well as remote analysis of condition state information on the policy management system 106.

[0125] Capabilities of the analysis engine also include the ability to query the policy data store 106B (Figure 1) to collect compliance policies and their associated value(s). This query could occur on a fixed periodic basis or be based on a specified system event, for example system startup, client startup, application start event, network interface event, authentication event, notification of received policy updates, receipt of a specific endpoint data element, receipt of a specific endpoint data element having a specific value, etc.

[0126] Capabilities of the analysis engine further include the ability to query the policy data store 106B to collect action policies and their associated value(s). This query occurs whenever needed by the analysis engine.

[0127] Capabilities of the analysis engine further include the ability to output status and event messages to local processes or remote computers accessible across a network. These messages may be used to trigger the display of a message to a user on the local endpoint system 104 user interface, the display of a message on the policy management system 106, the updating of status information on an already open display or may be logged to a local or remote data store for use in reports.

Endpoint Compliance Assessment Algorithms

[0128] With reference now to Figure 7, there is shown a process 700 for operation by policy management system 106 to determine whether endpoint system 104 is in compliance with the compliance policies maintained in data storage 106B, the process comprising an expansion of step 210 of Figure 2. In accordance with this process, condition data regarding the status of conditions 104F are collected through the above described system of agent managers and monitors, and input into analysis engine 106C through the processor and communications interface 106A (step 702). A compliance assessment process, or algorithm, is selected to process the condition data (step 704). Many different appropriate algorithms are described and shown herein below. Optionally, as described below, numeric risk values can be assigned to non-numeric condition state data and numeric weightings applied to numeric values (step 705). The effective and appropriate security policy is retrieved from data storage 106B (step 706), the condition data is processed using the selected compliance process (step 708), and the results of the processed condition data compared to the compliance policy (step 710). The details of this process, including the various algorithms, are described in detail herein below.

[0129] Because the policy action rules comprise a number of endpoint states that must be assessed, because there is a desire to be able to manage and change many policy settings using a finite number of data values and because of the number of possible combinations of endpoint states that could warrant invocation of the defined action, a simple rules based approach to processing this information may be unwieldy and not scale well. To facilitate the effective practice of the present invention, an algorithmic approach is provided by the present invention. As part of step 706 above, the algorithmic approach involves treating the non-numeric endpoint state information as real time values that are converted to numerical risk weightings, e.g. 1-100. Non-numeric endpoint state information, listed above, includes those states not communicated as a number, e.g. is an application running, what level of anti-virus program is running, etc.

[0130] The policy data store 106B contains a numeric value to assign to each non-numeric endpoint condition 104F. When the analysis engine 106C receives endpoint condition state information 104F from the agent monitors 104C, the analysis engine 106C

makes one or more queries to the policy data store 106B for each endpoint condition and retrieves the numeric value to assign to that particular endpoint condition. The process is repeated as needed for each non-numeric endpoint condition data element the analysis engine must convert from a non-numeric value to a numeric weighting. This process may also be repeated as needed for each numeric endpoint condition data element the analysis engine must convert from a raw numeric value to a normalized numeric weighting, e.g. converting the number of calendar days since antivirus was last updated (e.g. 0-365 days) to a normalized value in the e.g. 0-100 range.

[0131] This assignment of numeric weightings to non-numeric states allows effective analysis of the condition information using a wide range of numeric algorithmic models, and further allows non-numeric endpoint condition state information to be included and factored in when the analysis engine 106C is assessing policy compliance of endpoint condition state information that is already in numeric form. What follows are specific, but not exhaustive examples of specific algorithmic methods supported by the invention. Other numeric-based algorithmic methods within the scope of this invention will become apparent to the reader.

Matrix Analysis Algorithm

[0132] One analytical model operable by analysis engine 106C involves treating endpoint condition state information 104F as a matrix of numeric values where as mentioned above and as implied in each of the subsequent analytical models described herein, the real time state information is converted to numerical values or risk weightings, e.g. 1-100. The standalone and business intelligence rules can be treated as a second matrix where rules are given relative importance ratings. By combining the two matrices using conventional matrix mathematics, the analysis engine 106C generates a third matrix as the result. This third matrix contains numerical compliance scores that can be converted to security compliance ratings for different enforcement actions. Each rating can subsequently be compared to a predefined score threshold stored in the policy data store 106B for each possible enforcement action to determine whether or not to invoke the action. If the derived score is above the threshold, the endpoint is deemed sufficiently

(while not necessarily completely) compliant with those particular endpoint configuration policies.

[0133] The security score thresholds, the input matrix elements, the input matrix security scores and the items to be included in the endpoint inputs list are all data values stored in the policy data store 106B and as such are configurable and extensible so as to allow tailoring to an individual user's need. Configuration is performed using a user interface 106A, from which new or revised matrix elements, thresholds, weightings and factors can be created and modified. When implemented in a distributed fashion, changes to these data values made in the policy management system 106 can be distributed to the software agent residing on the endpoint system 104 using conventional software distribution methods. Examples of different matrix analysis methods are shown herein below.

Business Rules-Based Analytical Model for Policy Enforcement

[0134] One analytical model operable by analysis engine 106C in accordance with the present invention utilizes descriptive business rules. The rules specify a specific action to take if specified prerequisite conditions are true. When different system events and policy violations occur, different actions will be initiated. The universe of possible actions will expand and evolve over time, as will the tests used to determine whether a given action should be initiated. For example, new operating system services may come available, new categories of security or endpoint management applications may emerge, security point solutions may become integrated, transport technologies will continue to evolve, features of security point solutions will evolve, etc. Additionally, different operational needs will warrant creating new actions and new tests. This analytical model is extensible and allows the addition, removal, tailoring, and/or changing the values of prerequisite conditions or actions for different customers and policy groups. Note that this rules-based analysis may or may not require the assignment of numeric risk scores to non-numeric conditions, depending on the desired rules.

[0135] Examples of business rules used in this analytical model follow.

[0136] User Authentication Actions, including:

- Password reset action
 - Force password reset
 - When password age is greater than 90 days AND
 - When user is directly connected to corporate LAN AND
 - No policy violations exist that prevent connectivity to corporate LAN

[0137] Application Access Actions

- Application access block action:
 - Prevent named application from opening
 - When antivirus is out of compliance in any way
 - Prevent named application from opening
 - When antispware is out of compliance in any way
 - Prevent named application from opening
 - When antivirus is out of compliance in any way AND
 - When personal firewall is not running
 - Prevent named application from opening
 - If user is not connected to corporate LAN
 - Prevent named application from opening
 - If user is not connected to corporate LAN OR
 - If user is not connected from home
 - Prevent named application from opening
 - If any critical OS patches not found AND
 - If user not connected to corporate LAN AND
 - Antivirus not updated within last 212 days
 - Prevent named application from opening
 - If user not connected to corporate LAN AND
 - Day of week is Mon, Tues, Wed, Thurs or Fri AND

- Time of day is between 8 AM and 8 PM
 - Prevent named application from opening
 - If user not connected to corporate LAN OR
 - User does not have active VPN tunnel
 - Prevent named application from opening
 - If user authentication method anything other than RSA SecureID
- Application uninstall actions
 - Uninstall named application if found
- Application upgrade actions
 - Uninstall named application application if found AND
 - Retrieve named installation package from a named remote computer AND
 - Initiate installation of named installation package
- Application upgrade actions
 - If user is connected to corporate LAN AND
 - If approved antivirus client (vendor and version is not installed) THEN
 - Uninstall named application application if found AND
 - Retrieve named installation package from a named remote computer AND
 - Initiate installation of named installation package
- Restrict email application
 - When antivirus reports an infected system OR
 - Anti-spyware agent is not running
- Restrict HTTP applications such as web browsers
 - When local proxy setting is out of compliance, i.e. not configured for remote proxy server

[0138] File Management Actions

- Protect data:
 - Generate encryption key AND
 - Encrypt a specified file, files, folder or folders AND
 - Transmit encryption key to a policy-defined remote computer.

[0139] Hardware Devices Actions

- Launch Lojack application
 - When user fails authentication 100 successive times OR
 - When user attempts to copy encrypted data to USB port AND
 - Network connectivity exists over any transport
- Disable network adapter
 - When personal firewall is not running AND
 - Antivirus compliance score is less than 75% AND
 - Anti-spyware agent is not running

[0140] Network Access Actions

- Disconnect wireless adapter
 - When active wireless connection is ad hoc OR
 - When authentication method is not PEAP and 802.1x

Boolean Table-Based Analytical Model for Policy Enforcement

[0141] Another analytical model operable by analysis engine 106C in accordance with the present invention utilizes a table of Boolean logic rules. This will be understood to be an extension of the business rules-based model described above, with the inclusion of Boolean logic combinations. The rules specify specific actions to take when specified conditions are true. The universe of possible actions will expand and evolve over time, as will the tests used to determine whether a given action should be initiated. Additionally, different users may prefer different rules, new actions and/or new conditions to determine. This analytical model is extensible both in terms of inputs and actions and allows a user to add, remove, tailor, and/or change the values of inputs and/or actions for different systems.

[0142] An example of a policy table containing Boolean logic as used by this analytical model follows in Table 1.

Input 1	Input 2	Input 3	Action 1	Action 2	Action 3	Action 4
Antivirus Agent Running	Corporate Network Connection	Required OS Patches Installed	Allow Network Connectivity	Allow Email Application Access	Allow USB Ports	Alert IT Administrator
FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	TRUE
FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE
FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
TRUE	FALSE	TRUE	TRUE	TRUE	TRUE	FALSE
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE

Table 1

Scoring-Based Analytical Model for Policy Enforcement

[0143] Other analytical models supported by the present invention utilize different types of mathematical scoring methods. Endpoint state information collected by the agent can be assigned relative importance weightings or quantitative scores, as described above, to develop a composite security 'score' for the security dimension or dimensions associated with that endpoint attribute. The score can subsequently be used as a proxy for a numeric endpoint security health metric for a particular aspect of the endpoint's configuration or health. For example, an antivirus agent monitors the endpoint from a virus protection dimension and has certain attributes that must be in place to provide effective antivirus protection. Examples of attributes the antivirus agent must have in order to provide effective end point security and that is desired to be externally assessable state information to the invention includes:

- The antivirus agent must be running to provide any protection at all.
- The antivirus agent must be of a recent version to be able to recognize certain new virus patterns.

- The antivirus agent receives periodic virus signature updates used in the virus scanning and protection process. Frequent updates, or more precisely a recent update (which is assumed to have brought the antivirus agent fully up to date) is necessary to have protection against the latest threats.
- The antivirus agent has configuration settings that can be enabled or disabled to provide more or less protection.

[0144] Each of these attributes of the antivirus agent can be assigned an absolute score or a relative weighting by a user, based on the relative importance of that particular attribute to that user. For example as is shown in Table 2:

Agent Attribute	Points	Weight
Antivirus agent active and running	60	60%
Antivirus agent version current or current minus one rev	15	15%
Antivirus agent signature files updated within the last 212 days	100	100%
All antivirus scan options enabled	15	15%
Total	100	100%

Table 2

[0145] Different operators may have different views on the relative importance of these attributes and/or may wish to use different or more granular attributes in their scoring model. For example, a different user may want to replace the version attribute with a real-time file system monitoring enabled attribute or add this as an additional attribute in their scoring model. Similarly, another user may assign more relative importance, hence assign a higher weight or score to how recently the antivirus signature files were updated. Another user might want to assign each of 4 specific configuration settings 5 'points' if the setting is enabled, for a total of 20 possible points when all antivirus scans options of interest to that user are enabled.

[0146] These attributes may be different for different users depending on the capabilities of their particular endpoint security solution. For example, if a particular

commercially available antivirus agent has no configurable options to enable/disable, this attribute would not be relevant and would not be a consideration in the scoring process. In fact, one of the attributes could easily be the specific product being used, if a user has high confidence in 1-2 specific antivirus agents and much lower confidence in other antivirus agents. Support for variability across different end points having different hardware/software configurations is managed using policy settings as previously described.

[0147] Attributes and weightings can be similarly established for each of the endpoint security agents previously identified. The approach can similarly be adapted to other existing and future endpoint security solutions using this same approach.

Individual Agent Score Threshold Analysis and Enforcement

[0148] By establishing a minimum threshold for an agent and comparing the total agent score with that threshold, the total score obtained by querying the agent and/or its externally viewable attributes can be used as a trigger for one or more general or context-specific predefined actions to be taken. For example, assuming the following is the list of actions to be taken if the antivirus agent score does not meet or exceed a threshold of 81 points or 81%:

- Disable network interfaces so that the endpoint is prevented from connecting to a network
- Disconnect any active network connections, e.g. a dial, cellular or Wi-Fi connection
- Provide a user notification of the security state of the endpoint and instruct them to contact their help desk to resolve the issue.

[0149] A different operator may wish to take additional or alternative predefined actions, for example:

- Disable any active VPN connections
- Prevent the establishment of a VPN connection
- Apply an outbound access control list on the network protocol stack or using a personal firewall to limit outbound access to a specified set or one or more specific

application protocols (e.g. HTTP, POP, etc.), applications (e.g. Internet Explorer web browser, custom Oracle financial application, Symantec Norton Antivirus Update, BigFix Endpoint Vulnerability Management agent, etc.), network addresses (e.g. 192.1068.1.255), network numbers or subnets (e.g. 608.52.1022.0/206) and/or DNS domains (e.g. customer.com, macafee.net, server1.windowsupdate.com, etc.)

- Provide a user notification that outbound access is being restricted to specific applications, networks, etc. as appropriate as a result of the current security state of the endpoint.
- Activate a scripted remediation process to enable the antivirus agent if not running, update the antivirus signature files, enable all antivirus configuration settings, etc. as appropriate
- Once the remediation process is completed, reassess the antivirus score.
 - If score meets or exceeds threshold:
 - Remove VPN restriction
 - Remove outbound network access restrictions
 - Provide user notification indicating that endpoint security has now reached a satisfactory state and all normal system privileges have been restored
 - If score does not meet or exceed the threshold provide a user notification of the security state of the endpoint and instruct them to contact their help desk to resolve the issue.

[0150] A wide range of alternative system level corrective actions or user notifications are possible and may be more or less appropriate, depending on the situation and the user's needs. More complex conditional actions including IF, THEN, ELSE, AND, OR type logic may also be defined.

[0151] Note that in particular, the corrective actions may vary by agent. Thus for example, the corrective actions when the firewall agent score is below the firewall threshold might be:

- Disconnect any active network connection other than a wired Ethernet connection

- Prevent any network connections from being established other than a wired Ethernet connection
- Block outbound network access on the wired Ethernet connection unless the user's IP address is on the 1020.130.15.x network.
- IF the firewall is not currently running, THEN attempt to restart the firewall using a predefined command.
- Provide a context-sensitive user notification

[0152] Whereas for example the corrective actions when the antivirus agent score is below the antivirus threshold might be:

- Permit new network connections to be established
- Permit active network connections to remain active
- Prevent the following named applications from running:
 - Internet Explorer
 - Mozilla
 - Firefox
 - Opera
 - AOL
- Prevent the following file types from being opened:
 - .doc
 - .xls
- Upon detection of an active network connection send an antivirus update request message to a predefined URL
- Install the downloaded antivirus update package
- Provide user notifications regarding restricted applications
- Provide user status updates during the update process.

Composite Agent Scoring, Threshold Analysis and Enforcement

[0153] In the preceding examples, an antivirus agent was the single agent under evaluation. Multiple agents can be simultaneously assessed in a similar fashion and the

individual agent scores combined in different ways to create a holistic view of the endpoint state from multiple perspectives. For example, a user could define the following agent score combination logic as the basis for determining whether the end point is or is not in compliance:

- Antivirus agent score equal to or greater than 80% AND
- Firewall agent score equal to or greater than 90% AND
- Antispyware agent score equal to or greater than 50%

[0154] The individual agents of interest would be periodically queried or assessed at a configurable interval, individual agent scores calculated and then this business logic applied to determine if a noncompliance exists and if any predefined corrective, restrictive and/or notification actions (such as those previously defined) are required.

[0155] An alternative approach is to assign relative weighting to the individual agents, based on their relative importance to the user. For example as shown in Table 4 below:

Agent	Relative Points	Relative Weight
Antivirus agent	15	15%
Personal firewall agent	70	70%
Antispyware agent	100	100%
Content filtering agent	5	5%
Total	100	100%

Table 4

[0156] The relative weights for individual agents are then combined with the individual agent scores to derive a composite score. For example, as illustrated in Table 5 below:

Agent	Raw score (points)	Relative Weighting	Adjusted score (points)
Antivirus agent	65	15%	9.75
Personal firewall agent	93	70%	65.1
Antispyware agent	0	100%	0
Content filtering agent	100	5%	5
Composite Score			79.95

Table 5

[0157] In this approach, the composite score is 79.95 points or 79.95%. The composite score would then be compared to a predefined composite threshold residing as a data value in the policy data store 106B to determine if any predefined corrective, restrictive and/or notification actions (such as those previously defined) are required.

[0158] Different users may have different views on the relative importance of individual agents and may wish to use fewer, additional or different agents in their composite scoring model. For example, a different user may want to replace the content filtering agent with a patch management agent in their composite scoring model or add the patch management agent to the above composite scoring model. Similarly, another user may assign more or less relative importance, hence assign a higher or lower relative weight to the personal firewall. Such differences are accommodated by the invention through the use of policy settings and values that specify the agents of interest, the compliance thresholds, the relative weightings and other relevant considerations.

Complementary Individual & Composite Agent Scoring, Threshold Analysis and Enforcement

[0159] While the composite approach provides a comprehensive assessment of the endpoint state and can be the basis for automated notifications or corrective actions, it does not preclude automated notifications or corrective actions triggered by assessments of individual agent scores. Therefore composite corrective actions can be defined

independently of individual agent corrective actions (e.g. antivirus agent corrective actions, personal firewall corrective actions, etc.) if defined values exist in the policy data store 106B. For example, the previous composite example can be expanded as follows in Table 6:

Agent	Raw score (points)	Agent Threshold (points)	Relative Weighting	Adjusted score (points)
Antivirus agent	65	75	15%	9.75
Personal firewall agent	93	90	70%	65.1
Antispyware agent	0	70	100%	0
Content filtering agent	100	60	5%	5
Composite Score				79.95
Composite Threshold				75.00

Table 6

[0160] In this example, the overall composite score exceeds the composite threshold, thereby not requiring invocation of previously defined composite corrective actions. However, the individual score for the antivirus agent is below the antivirus threshold, thus requiring invocation of previously defined agent-specific antivirus corrective actions. Examples of corrective actions were previously defined above.

Single Level Versus Multi-Level Agent Scoring, Threshold Analysis and Enforcement

[0161] The previous examples (single agent assessments as well as composite assessment) all utilized a single threshold. In a single threshold model, when the score is below the threshold, corrective action is required and when the score is above the threshold, no corrective actions are required. This concept is readily extensible (for both single agent assessments and composite assessments) to a multi-level threshold model,

where different corrective actions exist at different score thresholds. Corrective actions to take for different score thresholds are stored as data values in the policy data store 106B. For example:

- Antivirus Agent Thresholds & Actions
 - 40%:
 - Prohibit the following applications from running:
 - Outlook
 - Outlook Express
 - Eudora
 - Thunderbird
 - Cisco VPN client
 - Nortel VPN client
 - Internet Explorer
 - Firefox
 - Block outbound POP protocol traffic
 - Restart antivirus if not running
 - Update virus signature files if greater than 15 days old
 - Enable realtime filesystem monitoring if not currently enabled
 - Prohibit all .doc and .xls files from opening
 - 60%:
 - Prohibit the following applications from running:
 - Cisco VPN client
 - Nortel VPN client
 - Update virus signature files if greater than 15 days old
 - Enable realtime filesystem monitoring if not currently enabled
 - 86%:
 - No restrictions
- Personal Firewall Agent Thresholds & Actions:
 - 55%:
 - Restart firewall if not running
 - IF local IP address is 1023.1023.1023.x AND IF endpoint is able to

send ICMP ping to host 1023.1023.1023.56, THEN permit only wired Ethernet access, ELSE block all outbound network access on all transports

- 91%:
 - No restrictions
- Composite Assessment Thresholds & Actions
 - 51%:
 - Prohibit the following applications from running:
 - Cisco VPN client
 - Nortel VPN client
 - Oracle financials
 - SAP payroll manager
 - Restrict HTTP access to the following domains:
 - Symantec.com
 - Windowsupdate.com
 - BigFix.com
 - Customer.com
 - Block outbound SMB protocol traffic
 - Block write access to the My Documents folder and all underlying subfolders
 - 75%:
 - Prohibit the following applications from running:
 - Cisco VPN client
 - Nortel VPN client
 - 85%:
 - No restrictions

Continuous Reporting Versus Exception Reporting Threshold Analysis and Enforcement

[0162] In each of the examples above, all collected data points are analyzed for compliance or given a compliance score that may be examined individually or included in a broader composite compliance assessment process. An alternative implementation is to not provide a value to a composite compliance assessment routine unless there is a compliance violation and have the composite compliance assessment routine assume that component is in compliance unless notified otherwise, i.e. utilize exception-based compliance notifications. In the example previously described:

Sensor	Raw score (points)	Agent Threshold (points)	Relative Weighting	Adjusted score (points)
Antivirus agent	65	75	15%	9.75
Personal firewall agent	93	90	70%	65.1
Antispyware agent	0	70	100%	0
Content filtering agent	100	60	5%	5
Composite Score				79.95
Composite Threshold				75.00

[0163] The individual raw scores for antivirus, personal firewall, anti-spyware agent, and content filtering must be fed into the composite scoring software process in order for the composite score to be determined. Conversely, in the exception-based model, the composite scoring software routine assumes the individual agent thresholds have been met, (e.g. the antivirus agent score is 75, the personal firewall agent score is 90, the anti-spyware agent score is 70 and the content filtering agent score is 60) unless informed otherwise. The exception when reported is used to update the composite score data set and a revised composite score is calculated. This exception-based approach is also supported by the invention.

[0164] Note also that the methods can be combined when so enabled via a policy setting. Continuing with the example above, the composite scoring software routine assumes that the antivirus agent score is 75 points and assumes the personal firewall agent score is assumed to be 90, unless otherwise notified. However the composite scoring software routine makes no assumption regarding the anti-spyware agent score or the content filtering agent score and requires that the antivirus compliance scoring software routine as well as the content filtering compliance scoring software routine both report actual raw compliance scores. Combinations of this type are also supported by the invention.

[0165] Different users may wish to have different sources utilize exception-based reporting and different sources utilize mandatory reporting. Such variations and adjustment capabilities are supported by the invention through the use of policy settings and values residing in the data store.

Matrix Algebra-Based Analytical Model for Policy Enforcement

[0166] Additional analytical models supported by the present invention utilize different matrix algebra methods. This model extends upon the scoring based analytical model previously described.

Matrix Method #1

[0167] In one matrix algebra method, different agents report different types of information regarding the state of the endpoint, such as:

- Antivirus agent
- Personal firewall
- Anti-spyware agent
- Endpoint vulnerability management
- Content filtering

[0168] While these agents monitor and inspect different aspects of the endpoint environment, from a policy compliance perspective, there are common policies or target states of interest across each of these data sources, such as:

- Whether the agent is running
- Whether it is a desired or required vendor
- Whether it is up to date with signature updates
- Whether it is configured correctly or optimally

[0169] Relative weights regarding the importance of compliance for each attribute can be assigned for each monitored condition. The collection of information can then be represented in tabular form in anticipation of making the data available for matrix algebra or other linear and nonlinear analysis methods. For example, the following Table 7 shows how one operator has identified 3 data sources of interest, identified 3 attributes of interest, and assigned levels of relative importance to each data source/attribute pairing. These data sources, attributes and values are stored in the policy data store. The policy data store also contains the specific target values or thresholds for each of these attributes, e.g. the desired antivirus agent is product XYZ, the maximum age in days of the most recent anti-spyware agent is 30 days, the required configuration settings and values for the personal firewall are: no inbound access permitted, outbound access using HTTP protocol permitted, etc.

Data Source	Agent From Approved Vendor Currently Running	Updated Within X Days	Required Configuration Settings Enabled	Total
Antivirus agent	80	15	5	100
Personal firewall agent	60	20	20	100
Antispyware agent	70	25	5	100

Table 7

[0170] It will be apparent to the reader that fewer, alternative and/or additional data sources could be used instead of those shown above. Obviously, fewer, alternative and/or additional attributes could be used instead of those shown above.

[0171] When the real time or periodic measurement of a given condition is in compliance relative to the security policy, all possible points are awarded. When a given condition is not in compliance relative to the policy, no points are awarded.

[0172] In the following example:

- The antivirus agent is running, is from an approved vendor and has been updated recently. However one or more critical configuration settings are not set correctly.
- The personal firewall agent is running, is from an approved vendor, has been updated recently and has configuration settings set correctly. However it has not been updated in the past 21 days.
- There is no anti-spyware agent running on the endpoint (and possibly is not even installed on the endpoint).

[0173] The resulting matrix that represents the current state of the endpoint is as follows:

Data Source	Agent From Approved Vendor Currently Running	Updated Within 21 Days	Required Configuration Settings Enabled	Total
Antivirus agent	80	15	0	95
Personal firewall agent	60	20	20	100
Antispyware agent	0	25	5	212

[0174] As this is an $n \times n$ matrix, the matrix determinant can be calculated using the following Formula 1:

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} = a_1 b_2 c_3 - a_1 b_3 c_2 - a_2 b_1 c_3 + a_2 b_3 c_1 + a_3 b_1 c_2 - a_3 b_2 c_1.$$

$$=-36,500$$

Formula 1

[0175] The determinant derived from assessing the current state of the endpoint can be compared against a minimum threshold defined in the policy data store 106B that must be met in order for the endpoint to be considered in compliance.

Matrix Method #2

[0176] The matrix method described above can be further extended by assigning relative weightings to the data sources, treating the resulting values as a row or column vector matrix, and performing matrix multiplication of the data source relative importance matrix and the current state matrix. This allows the evaluation of compliance in a given dimension or attribute across a number of data sources, factoring in the relative compliance importance of the different data sources.

[0177] For example the following vector shows how the relative weights of these data sources assigned by one user:

- Antivirus agent: 20%
- Personal firewall agent: 70%
- Anti-spyware agent: 10%

[0178] This relative weighting can be represented as a matrix row vector: A = [0.2,0.7,0.1].

[0179] The relative weighting matrix and the current state matrix are multiplied using conventional matrix algebra to yield:

$$\begin{bmatrix} 0.2 & 0.7 & 0.1 \end{bmatrix} \times \begin{bmatrix} 80 & 15 & 0 \\ 60 & 20 & 20 \\ 0 & 25 & 5 \end{bmatrix} = \begin{bmatrix} 16.0 & 19.5 & 14.5 \end{bmatrix}$$

[0180] Therefore, the current assessment of the endpoint's overall compliance using these sample data sources, sample relative data source weightings, sample data sources attributes, and current state values are:

- Security applications current running using approved vendor agents compliance score: 16.0
- Security applications recent updates compliance score: 19.5
- Security applications current configuration compliance score: 14.5

[0181] These compliance scores are compared to policy-defined thresholds in order to make a compliance assessment. For example assume the following values exist for these policies in the policy store:

- Required current running security agents with approved vendor compliance score: 20.0
- Required security agent software and signature files currency compliance score: 15.0
- Required security agent current configuration compliance score: 10.0

[0182] In this situation, the endpoint is out of compliance with regards to currently running security agents and their vendor, in compliance with regards to current configuration settings, and in compliance with regard to configuration settings.

[0183] It will now be apparent to the reader that these methods can be extended and/or modified in a number of ways with regards to the data sources, attributes, data source relative weightings, attribute relative weightings, compliance thresholds, etc.

Context-Sensitive Threshold and Weighting Adjustments to Quantitative Analytical Models for Policy Enforcement

[0184] In any of the numeric-base methods supported by the client, examples of which are shown above, scores, thresholds, weightings, etc. may be scaled up or down using a global weighting adjustment or discrete weighting adjustments stored as policy values in the policy data store. Similarly, situation-specific policy-based adjustments can be made to scores and thresholds for other analytical models that may be added to the policy management system in the future.

[0185] For example, a user directly connected to the corporate network likely benefits from levels of protection or compliance monitoring systems integrated by the employer into the local network, reducing the criticality that one or more security applications are running or correctly configured on the user's machine. Therefore, an administrator may wish to relax the minimum compliance score required to be able to access the corporate network, or specific computers and/or applications on the corporate network by a number of points. In this situation, the analysis engine would query the policy data store for the minimum compliance score required to allow a certain system event to occur, determine the user's location (e.g. on the corporate network or not), if on the corporate network determine if the minimum compliance threshold should be adjusted by retrieving the policy value for the on-campus network security adjustment policy, adjust the compliance threshold as necessary, and then finally assess the compliance state of the endpoint using this adjusted threshold.

[0186] Other policy-based, situation-specific or context-sensitive adjustments are possible based on endpoint state information and such adjustment capabilities are supported by the policy management system.

Statistics-Based Analytical Model for Policy Enforcement

[0187] Additional analytical methods supported by policy management system 106 are based on statistical analysis methods. These methods differ from methods previously described herein in that compliance analysis methods described below are based on evaluation of a population sample comprised of multiple data points collected over a period of time, rather than a evaluation of a single collected data point.

[0188] As an illustrative example of single data point methods previously described herein, the policy management system 106 can be configured via a policy setting within policy store 106B to query the operating system or an external agent within endpoint 104 every X seconds, where X is a policy-defined value (e.g. interval in seconds = 60) to determine the value of any system metric, e.g. CPU utilization. This value can be passed immediately to the compliance analysis engine upon collection as an indicator of the instant CPU utilization. In this case, the sample size is one. The following examples illustrate several of the methods the client supports for utilizing larger sample sizes to assess compliance with regards to CPU utilization.

[0189] The ability to apply these methods to other measurable metrics on the endpoint are capabilities of the policy management system. While the examples cited here utilize CPU utilization as the metric under evaluation, the same capabilities and options can be readily applied to any other numeric endpoint metric including but not limited to:

- Network bytes received
- Network bytes transmitted
- Physical memory in use
- Queries to virtual memory
- Free virtual memory
- Transaction response time for specific application transactions
- Number of times a specific application transaction occurs
- Number of times an application is opened
- Emails sent
- Emails received
- Email arrival rate (e.g. emails arriving per minute)
- Email reception rate
- Email attachment count
- Email attachment size
- Number of recipients in emails sent

- DNS queries
- DNS queries serviced by local DNS cache
- ICMP messages transmitted
- ICMP messages received
- HTTP requests sent
- HTTP request transmission rate
- File open rate (e.g. files opened per minute)
- Etc.

[0190] Additionally, as described previously herein, the analysis engine 106C is able to apply these methods to ratings or scores that are derived from inspecting numeric or non-numeric attributes of the endpoint, evaluating their state, comparing the current state with policy values that define numeric weightings or scores for a given state of a given endpoint attribute, and assigning a numeric value to that state. The assigned numeric value then becomes one data sample of a sample population.

Data Summary-Based Statistical Analysis Methods

[0191] The analysis engine 106C is able to utilize statistical analysis methods for assessing compliance against a single, related group or arbitrary group of numeric conditions for the purposes of calculating a central tendency value of raw (i.e. reported directly from one of various exemplary agents 104E) and/or computed (i.e. normalized by passing raw numeric or non-numeric condition identifiers and values to the analysis engine 106C and having the analysis engine query the policy data store 106B to determine the appropriate score to apply to the raw numeric or non-numeric value) condition(s), comparing the calculated value to corresponding policy values residing in the policy data store 106B that define compliance value(s) and/or ranges for the data element(s), and making an assessment about compliance of that/those data element(s). The central tendency of a value given a sample population is commonly termed an 'average', however that is a general term and there are in fact several statistical analysis methods for calculating the central tendency of a sample population. The analysis engine 106C does in fact support several methods as described below. The specific method used

for calculating the central tendency value of a given data element is selected by the operator. It will be apparent to the reader that the nature of the distribution makes certain methods more or less appropriate or optimal.

[0192] Specific averaging methods supported by the analysis engine 106C include the following.

Mean-Based Analysis Method

[0193] Using an average (or mean) statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 5) at a policy-defined sampling interval (e.g. interval = 60 seconds) and then calculate an average or mean value over the consecutive data samples. The average or mean value is determined by summing the values of the collected samples and then dividing the sum by the number of samples. This calculated average or mean is the value passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses. An updated average or mean is passed to the compliance assessment routine at a frequency roughly equivalent to the sampling window size, immediately following calculation of the mean.

Moving Average-Based Statistical Analysis Method

[0194] Using a moving average statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 5) at a policy-defined sampling interval (e.g. interval = 60 seconds) and then calculate an average or mean value over the consecutive data samples. The average or mean value is determined by summing the values of the collected samples and then dividing the sum by the number of samples. This calculated average or mean is the value passed to the compliance assessment process at the completion of the sampling window and used in subsequent compliance analyses. An updated average or mean is passed to the compliance

assessment routine at a frequency roughly equivalent to the sampling interval, immediately following calculation of the moving average over the last X samples.

Median-Based Statistical Analysis Method

[0195] Using a median statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 5) at a policy-defined sampling interval (e.g. interval = 60 seconds) and then determine the midpoint between the highest and the lowest value among all the collected samples. This median value is the value passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses.

Mode-Based Statistical Analysis Method

[0196] Using a mode statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 5) at a policy-defined sampling interval (e.g. interval = 60 seconds) and then determine the value that occurs most frequently among all the collected samples. This mode value is the value passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses. In the event that no mode value exists, which is possible if all values in the sample population are equal, the compliance analysis engine will pass the average or mean value to the compliance assessment routine at the completion of the sampling window.

Geometric Mean-Based Statistical Analysis Method

[0197] Using a geometric mean statistical analysis method, the compliance analysis engine is configured to perform a system query, e.g. for TCP segment window size a policy-defined number of times, (e.g. count = 5) at a policy-defined sampling interval (e.g. interval = 60 seconds) and then determine the geometric mean of the rate of change. For example, when a new TCP connection is opened between the endpoint and a remote

server application across the network, the measured values of the segment window size in successive samples might be as follows:

- Sample 1: 604 bytes:
- Sample 2: 72 bytes (increase of 12.5%)
- Sample 3: 100 bytes (increase of 38.89%)
- Sample 4: 150 bytes (increase of 50%)
- Sample 5: 250 bytes (increase of 606.67%)

[0198] In this case the geometric mean is
$$[1.125 \times 1.3889 \times 1.5 \times 1.6667]^{1/4} - 1 = 0.4058 = 40.58\%$$

[0199] This geometric mean value is the value passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses.

Rate-Based Statistical Analysis Method

[0200] Using a rate-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, CPU temperature, number of emails sent, antivirus agent compliance score, personal firewall compliance score, composite security score, etc.) two times at a policy-defined sampling interval (e.g. interval = 100 seconds). The analysis engine performs a calculation of the difference between the two sampled values (or calculated compliance scores), performs a calculation of the difference between the two sampling times (or alternatively uses the policy-defined sampling interval), and divides the value difference by the time difference to obtain a rate, e.g. emails per second, change in CPU temperature per second, number of HTTP requests to a given DNS domain per minute, change in antivirus compliance score per minute, authentication failures per minute, etc. This rate value is the value passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses. This rate calculation result can also be used by the client to predict the value of the data element (either raw data or calculated score) at a future time. This predicted value can be used in subsequent compliance analysis. It will be understood that rates can be determined from many other sampling processes.

Acceleration Rate-Based Statistical Analysis Method

[0201] Using an acceleration rate-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, CPU temperature number of emails sent, antivirus agent compliance, etc.) two times at a policy-defined sampling interval (e.g. interval = 100 seconds). The compliance analysis engine performs a calculation of the difference between the two values, performs a calculation of the difference between the two sampling times (or alternatively uses the policy-defined sampling interval), and divides the value difference by the time difference to obtain a rate (e.g. emails per second, change in CPU temperature per second, number of HTTP requests to a given DNS domain per minute, change in antivirus compliance score per minute, authentication failures per minute, etc. Rather than passing this value to the compliance assessment routine at the completion of the sampling window as described in the previous method, the compliance analysis engine repeats this activity at a later time, where the time interval between the first rate sampling window (which collects two samples at a policy-defined sampling interval) and the second rate sampling window (which collects two additional samples at the same policy-defined sampling interval) is defined as an acceleration policy setting in the client policy data store.

[0202] The compliance analysis engine performs a calculation of the difference between the two rate values, performs a calculation of the difference between the two sampling times (or alternatively uses the policy-defined acceleration sampling interval), and divides the value difference by the time difference to obtain a change in rate per unit time (i.e. just as the physical property acceleration is the measurement of change in *velocity* per unit time, where velocity itself is the measurement of the change in distance (the raw value being measured) per unit time. This acceleration value is the value passed to the compliance assessment routine at the completion of the acceleration sampling window and used in subsequent compliance analyses. This acceleration calculation result is also able to be used by the client to predict the value of the rate at a future time. This predicted value can be used in subsequent compliance analysis.

Variability-Based Statistical Analysis Methods

[0203] The compliance analysis engine is able to utilize statistical analysis methods for assessing compliance against a single, related group or arbitrary group of data elements for the purposes of calculating the variability value of raw, computed and/or mapped data element(s), comparing the calculated variability value to corresponding policy values that define compliance value(s) and/or ranges for the data element(s), and making an assessment about compliance of that/those data element(s).

[0204] Specific variability methods supported by the client are set out below. The specific method that should be used for calculating the variability value of a given data element or combination of data elements is selected by the administrator, as the nature of the distribution makes certain methods more or less appropriate or optimal for evaluating compliance of a given data element or combination of data elements.

Min-Based, Max-Based and Range-Based Statistical Analysis Method

[0205] Using a minimum, maximum or range-based statistical analysis method, the client is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 5) at a policy-defined sampling interval (e.g. interval = 60 seconds) and then determine the minimum and maximum values that were observed in the collected sample. If range information is necessary, the client will also calculate the range based on the observed minimum and maximum. The minimum, maximum and/or values are passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses.

Variance-Based Statistical Analysis Method

[0206] Using a variance-based statistical analysis method, the client is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 100 seconds) and then determine the variance of the collected sample using a standard formula for calculating sample variances:

$$s^2 = \frac{1}{n-1} \times \sum_{i=1}^n (x_i - \bar{x})^2 \quad \text{where} \quad \bar{x} = \frac{1}{n} \times \sum_{i=1}^n x_i$$

[0207] The calculated variance is passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses.

Standard Deviation-Based Statistical Analysis Method

[0208] Using a standard deviation-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 100 seconds) and then determine the standard deviation s of the collected sample, where the standard deviation is equal to the square root of the variance. The method for calculating the variance was just described in the preceding variance-based statistical analysis method description

[0209] The calculated standard deviation is passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses.

Coefficient of Variation-Based Statistical Analysis Method

[0210] Using a coefficient of variation (COV)-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 100 seconds) and then determine the COV of the collected sample using a standard formula for calculating COV:

$$COV = \frac{\text{Sample Standard Deviation}}{\text{Sample Mean}}$$

[0211] Where the sample standard deviation is equal to the square root of the sample variance, and where the sample variance is equal to:

$$s^2 = \frac{1}{n-1} \times \sum_{i=1}^n (x_i - \bar{x})^2 \quad \text{where} \quad \bar{x} = \frac{1}{n} \times \sum_{i=1}^n x_i$$

[0212] And where the sample mean is determined by summing the values of the collected samples and then dividing the sum by the number of samples.

[0213] The calculated COV is passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses.

Number of Occurrences-Based Statistical Analysis Method

[0214] Using a number of occurrences-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 1 second) and count the number of occurrences of each different value collected. The list of values and their frequency of occurrence is then passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses. This method is useful in situations where the action policy is triggered based on the number of occurrences of a specific value or values of a given data element in a sampling window.

Occurrence Frequency-Based Statistical Analysis Method

[0215] Using a percentage of occurrence-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 1 second) and count the number of occurrences of each different value collected. The number of occurrences of a given value is divided by the number of samples to determine the relative frequency of occurrence of that value. This will normally be expressed as a decimal value or a percentage. The list of values and their frequency of occurrence is then passed to the

compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses. This method is useful in situations where the action policy is triggered based on the relative frequency of occurrences of a specific value or values of a given data element in a sampling window.

Cumulative Distribution-Based Statistical Analysis Method

[0216] Using a cumulative distribution-based statistical analysis method, the compliance analysis engine is configured to perform a system query (e.g. CPU utilization, antivirus agent compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 1 second), sort the collected samples in ascending order, count the number of occurrences of each different value collected and determines the relative frequency of each value as described above. The compliance analysis engine then calculates the cumulative frequency distribution of each value by adding the relative frequency of that value to the sum of the relative frequencies of all lesser values. The list of values and their cumulative frequency of occurrence is then passed to the compliance assessment routine at the completion of the sampling window and used in subsequent compliance analyses. This method is useful in situations where the action policy is triggered when the relative cumulative frequency exceeds a policy-defined threshold. For example, analysis of a sample of 100 transactions of type X concludes for this population sample that 90% of the transactions completed within 3.5 seconds. This result is compared to a predefined policy in the policy data store that specifies that 90% of type X transactions must complete within 4 seconds to determine whether or not a condition exists that warrants taking a policy-defined action on the endpoint.

Sampling Distribution-Based Statistical Analysis Method

[0217] Using a sampling distribution-based method, an administrator may measure successive values of a data element of interest a large number of times in either a controlled or typical endpoint environment to determine the distribution type, mean, variance and standard deviation of the values of that data element. Alternatively an administrator may define a target mean and standard deviation he believes reasonably

describes the distribution of the values of the data element of interest. These values are stored in the client policy data store as policy values such that they can be changed in the future as needed.

[0218] Alternatively a policy can be enabled in the compliance analysis engine that causes the compliance analysis engine to monitor a particular data element for a period of time until a sufficiently large sample to accurately represent the population of possible data values is collected, and then calculate a mean and standard deviation for the very large sample. These values also can be stored in the client policy data store as target policy values that represent the steady state behavior of that particular data element. The monitoring and data collection activity performed by the client can be started or stopped at any time using policy settings or commands issued to the client. The calculated properties (e.g. mean, standard deviation, etc) can be discarded at a policy-defined interval (e.g. every 60 days) or date (e.g. 12/31/05) and the procedure repeated, such that the client periodically refreshes the values stored in the policy data store that describe the population.

[0219] These values can further be used to calculate the probability of a sample event having a value greater than a specified policy value, less than a specified policy value, or within a specified range of policy values. This capability is supported in the client by transforming the sample value into a normal random variable with mean equal to zero and a variance of one. This transformation is done by subtracting the population mean specified value and dividing the result by the population standard deviation. The client includes a standard normal distribution data table in its local data store for looking up the probability of a given value or range of values of this transformed or normalized random variable.

[0220] The compliance analysis engine also allows an administrator to specify a mean and/or variance threshold relative to the population's mean and/or variance for a given value of a given data element or group of data elements. The compliance analysis engine can be configured to perform a system query (e.g. CPU utilization, antivirus agent

compliance, etc.) a policy-defined number of times, (e.g. count = 100) at a policy-defined sampling interval (e.g. interval = 1 second). The mean, variance and/or standard deviation of the sample can be calculated using standard methods such as those previously described. The calculated properties of the sample (e.g. mean, standard deviation) are then passed to the compliance assessment routine at the completion of the sampling window and compared by the compliance analysis engine to the policy-defined values that describe the population and that were previously defined by the administrator or calculated by the client. This method is useful in situations where the action policy is triggered when the properties of a sample, e.g. the mean or standard deviation, exceeds a policy-defined threshold. For example, the client locally observes a population sample of 100,000 events of a particular type, calculates the mean and the standard

Linear Regression-Based Analysis Method

[0221] Using a linear regression-based method, an administrator may measure successive values of an (x, y) data pair of interest comprised of an independent and a dependent variable. The measurement may occur a large number of times in either a controlled or typical endpoint environment to determine the coefficients (a, b) of a line equation that represents the relationship between the dependent variable (y) and the independent variable (x) using the standard line equation $y=ax+b$. Alternatively an administrator may define target coefficients he believes reasonably describes the fitted relationship of the values of the data pair of interest. These values are stored in the client policy data store as policy values such that they can be changed in the future as needed.

[0222] When the required number of samples is collected, the administrator utilizes the method of least squares for estimating the regression coefficients (a, b) of a line equation that represents the relationship between the dependent variable (y) and the independent variable (x) using the standard line equation $y=ax+b$, where

$$b = \frac{n \sum_{i=1}^n x_i y_i - \left[\left(\sum_{i=1}^n x_i \right) \times \left(\sum_{i=1}^n y_i \right) \right]}{n \sum_{i=1}^n x_i^2 - \left(\sum_{i=1}^n x_i \right)^2}$$

and where

$$a = \frac{\sum_{i=1}^n y_i - b \sum_{i=1}^n x_i}{n}$$

[0223] These values are then stored as policy values.

[0224] There are several analyses methods supported by the client that can subsequently make use of these policy values. In one method supported by the compliance analysis engine, the compliance analysis engine is configured to perform a system query of a data pair of interest (e.g. response time as a function of number of bytes or records in transaction request, number of network messages transmitted per minute as a function of number of active programs, etc.) a policy-defined number of times, (e.g. count = 50) at a policy-defined sampling interval (e.g. interval = 1 second) or when the event actually occurs, (e.g. a message being sent to a specific remote computer). A mathematical analysis is performed to calculate the actual regression coefficients of the sample. The calculated coefficients of the sample are then passed to the compliance assessment routine and compared by the client to the policy-defined values. A compliance assessment is subsequently made.

[0225] In another method supported by the compliance analysis engine, the policy-defined coefficients are combined with the sampled value of the independent variable (x) to determine an estimated value of the dependent variable (y). The actual value of the dependent variable (y) is then compared to the estimated value of the dependent variable (y). If the actual value differs from the estimated value by more than a specified, policy-

defined difference (positive, negative and/or absolute magnitude), a policy violation is deemed to have occurred.

[0226] In another method supported by the compliance analysis engine, the actual regression coefficients of the sample are used to predict the value of the dependent variable given a value of the independent variable. The predicted value of the dependent variable can then be used as a dynamically derived policy value. Should the specified value of the independent variable occur in the future, the actual value of the dependent variable at that time is compared by the compliance analysis engine with the dynamically derived policy value. If the actual value differs from the predicted value by more than a specified, policy-defined difference (positive, negative and/or absolute magnitude), a policy violation is deemed to have occurred.

Filtering Analysis

[0227] Another analytical method supported by the client is based on filtering theory. A filter in this context is a piece of purpose-built software that analyzes a particular data set, applies a threshold function of some type to that data set, and extracts only information of interest. Filtering in this context therefore is the act of extracting interesting data by applying a threshold against individual data points within a data set. Examples of the types of data the client can collect and policy-based thresholds the client can evaluate were previously described above.

[0228] The compliance analysis engine supports several different filtering approaches and is extensible to support future additional filtering approaches as well. One supported filtering method previously described involves by collecting a specific type of data from the environment, comparing the data point against policy-defined thresholds, and taking a policy-based action when a compliance threshold is exceeded.

[0229] In another filtering method supported by the client, the compliance analysis module assumes a particular aspect of the endpoint is in compliance unless otherwise notified by the data collection module. In this filtering approach, the filtering method

continuously collects a specific type of data from the environment and performs a comparison of that single point of data against the policy-defined threshold for that single point of data. Only when a compliance violation is detected, is the data, or alternatively a descriptive message identifying the compliance violation, passed to an alternate compliance analysis engine responsible for combining the results of assessments of individual data points, i.e. performing a holistic compliance assessment. The overall compliance analysis module assumes complete compliance with respect to any given data element unless it is informed otherwise. This is commonly referred to as an exception-based notification system. It is an advantageous approach as the software routine responsible for determining overall assessment has to process less data and thus can more quickly reach decisions with respect to required policy enforcement actions.

[0230] In a statistical approach to smoothing and prediction, there must be certain statistical parameters available such as a mean function or a correlation function. In particular, there must be a difference between the values of these functions for the interesting information and the function values for the noise. The filter is set to pass interesting information and filter noise by setting the filtering level appropriately.

Application of Methods to All Endpoint State Data Elements

[0231] Many of the examples of analysis methods described herein for measuring quantitative endpoint state information utilize one or two endpoint data elements (e.g. CPU utilization, antivirus agent compliance score) as an example. These same data elements are cited as examples throughout simply for reader convenience, and the reader will realize that the invention is not thus limited. The policy management system fully supports the ability to apply these methods to any number of endpoint data elements, either raw or derived as a result of an upstream compliance assessment and calculation performed by the policy management system.

Application of Methods to Non-Numeric Endpoint State Information

[0232] The above-described models and methods for measuring quantitative endpoint state information can be applied to non-numeric compliance assessments by mapping the environmental data to numeric values using policy-defined values, as noted above.

[0233] As an example, the state of the antivirus agent and a review of policy settings might result in an antivirus compliance score of 65 points or 65%. Rather than treat this as a single data point and form an immediate compliance assessment, it might be preferable to sample the antivirus agent state information at a periodic interval for a period of time, where both the sampling interval and sampling window are policy-defined values, calculate the compliance score at each sampling, and treat the collection of compliance scores as a population sample. Such capabilities are supported by the policy management system. While this example cites the translation of antivirus agent state information into an antivirus compliance score, translation of other endpoint state information such as those data elements previously identified herein into compliance scores is also supported by the present invention. Collection of population samples of numeric compliance scores for other pieces of endpoint state information is likewise supported by the present invention.

Application of Analytical Methods to Composite Endpoint Compliance Assessments

[0234] Just as statistical and other analytical methods can be applied to compliance assessments of discrete data elements (e.g. CPU utilization) or data sources (e.g. antivirus agent state including version, running state, vendor, date of last signatures update, configuration settings, etc.), these methods can also be applied to composite compliance assessments.

[0235] In a previous example, the real time compliance assessment at a given point was as follows:

Sensor	Raw score (points)	Agent Threshold (points)	Relative Weighting	Adjusted score (points)

Antivirus agent	65	75	15%	9.75
Personal firewall agent	93	90	70%	65.1
Antispyware agent	0	70	100%	0
Content filtering agent	100	60	5%	5
Composite Score				79.95
Composite Threshold				75.00

[0236] As previously mentioned, the policy management system is able to use statistical and other analysis methods to calculate one or more raw score inputs into this composite score.

[0237] The policy management system is also able to use statistical analysis methods cited above, including but not limited to mean, median, mode, moving average and geometric mean to calculate a composite score by applying a statistical analysis method to a population sample of individual composite scores calculated at different times. Sampling intervals and sample count are controlled via policy settings. The policy management system is able to perform this function using all of the statistical analysis methods previously described. The client is able to perform this function for all monitored data elements and all composite scoring functions.

Exception Reporting of Analyses Result

[0238] Recalling the exception-based optional approach previously described, in another embodiment the instant CPU utilization, the average CPU utilization, or moving average CPU utilization can be reported every time the value is determined, or only reported when it exceeds a policy defined threshold.

Non-Exclusivity of Analyses Methods

[0239] In the examples cited, the instant CPU utilization, average CPU utilization, moving average, etc. are distinctly different data elements, however the different data elements can be used simultaneously for different compliance evaluation purposes, i.e. collection and usage of instant CPU utilization and average CPU utilization are not mutually exclusive. For example, one compliance evaluation method may require the instant CPU utilization value in order to perform a compliance evaluation, whereas a different compliance evaluation method may simultaneously require the average CPU utilization in order to perform a compliance evaluation. The present invention supports the ability to use these different measurement methods for different compliance tests using the same data source simultaneously. The present invention further supports this simultaneous use capability for all other supported monitored data sources as well, including both numeric sources and non-numeric sources that are converted to numeric values or scores.

Combining Analyses Methods

[0240] In the examples cited herein, average, mode, moving average, coefficient of variation, standard deviation, etc. are different analysis methods supported by the policy management system. It will be understood that the policy management system provides the ability to use logical combinations (e.g. AND, OR, ELSE, IF, THEN, NOT, etc.) of different compliance measurement methods for performing compliance evaluation of the same data element or group of data elements simultaneously. Examples of policy-driven capabilities of the policy management system include:

- CPU utilization policy: Median of past 100 consecutive samples must be less than 98% AND trailing 5 minute moving average must be less than 80%
- File open rate policy: Mean of past 5 consecutive samples must be less than 100 AND standard deviation on those same samples must be less than 7.
- Antivirus compliance policy: Most recent calculation of antivirus compliance based on most recent antivirus state inspection must have a compliance score greater than 50 OR mean of past 5 consecutive samples must be greater than 70.

[0241] The policy management system supports this simultaneous use capability for all other supported monitored data elements as well, including both numeric sources and non-numeric sources that are mapped to numeric values or scores.

[0242] Similarly, it is important to note that simultaneously used combinations of these methods, as well as other methods cited herein are possible and are supported by the policy management system. For example, the business rules method cited previously could be used for compliance monitoring and enforcement with regards to physical ports on the endpoint, such as USB ports, serial ports, printer ports, IR or RF communication ports, etc., while the Boolean rules method cited previously could be used for compliance monitoring and enforcement with regards to permitted applications, while a matrix algebra method could simultaneously be used for compliance monitoring and enforcement with regards to network connectivity or VPN tunnel establishment. Other combinations are of course possible as well. These combinations are considered in accordance with one of the above-described methods, for example in Boolean combinations or as otherwise described herein. Such combinations are also supported by the policy management system.

Real Time Adjustment of Sampling Frequency

[0243] When an endpoint is compliant with security policies, a reduction in endpoint inspection frequency reduces the load on the system, e.g. memory, file access, etc. Conversely, when an endpoint is out of compliance, and in particular when certain critical security situations exist, it is appropriate to inspect the endpoint with much higher frequency so that a highly up-to-date view of the endpoint's state exists at all times. Therefore condition data relating to monitored items (e.g. CPU utilization, antivirus compliance score, security agents composite compliance score, etc.) can be collected at different sampling intervals, for thresholds (or the range) above which or below which the new sampling frequency parameters take effect. The policy management system provides the ability to support this very capability through the use of policy settings where these parameters can be specified and configured.

Managing Endpoint and Host Operation

[0244] Continuing with reference to Figure 2, when policy violations are detected it may be desired to take one or more discrete actions to either bring the endpoint into compliance, prevent harm from coming to the local and/or remote computers, restrict user actions, or perform any number of different actions (step 212). Examples of discrete actions which may be initiated by policy management system 106, and executed by host system 102, and endpoint system 104, include those set out below. The solution is extensible to allow additional actions to be added in the future and configurable to allow different groups to customize different actions to best meet their needs. It will be understood that the process of managing the endpoint and host operations repeats as frequently as necessary (step 214). As noted herein above, it may be desirable to repeat the steps, including the collection of data, analysis of data, and the management of the systems, multiple times during a single connection session.

[0245] With reference back again to Figure 4, there is shown how the above described operation of compliance analysis engine 106C results in the generation of output actions 402, these actions used to control the operation of the agents within the endpoint. These policy actions are selected based upon the above-described comparison of the state of the conditions 14F in comparison to the compliance rules in data store 16B, and specify actions to permit, prevent or automatically initiate on the endpoint. Policy actions may be endpoint actions allowed to take place because the endpoint system 104 is in compliance with security policies, actions to take to partially or wholly restrict access to endpoint resources because the endpoint system 104 is not in compliance with security policies, or a combination thereof. Additionally, the invention may log event information locally in the policy data store and/or create and transmit event and state information across a data communications network to a remote policy management system 106 or a remote computer for logging, operator notification, transaction triggering, reporting, or other administrative purposes. Figure 4 in particular illustrates the notion of endpoint agent closed loop control feedback as a central part of the invention where endpoint policy actions taken may be targeted to a one or more specific endpoint agents 104E as a direct result of endpoint condition information 104F obtained from that endpoint agent

104E and other various exemplary agents. For example the antivirus agent may be queried for its current state. That information may then be combined with other information from other endpoint agents and analyzed by the analysis engine 106C to determine if any noncompliance conditions exist. If so, the invention may direct the antivirus agent to take specific actions, change internal configuration settings, etc. to bring the endpoint back into compliance or to block or permit certain system or operator activities.

[0246] Examples of specific endpoint policy actions the invention is able to take are itemized previously in this document. Additional examples of endpoint actions the invention is able to take are now shown:

- Certificate Actions
 - Grant or deny access to a locally stored digital certificate
 - Transmit a certificate revocation request message
- Login Account Actions
 - Disable login account
 - Expire password
 - Initiate password reset
 - Automatically log a user out of an application, the system, a secure connection, etc.
- Operating System Actions
 - Halt a named memory-resident process
 - Delete a specific file
 - Rename a specific file
 - Change the attribute of a file from read/write to read only, or reverse
 - Change the attribute of a folder from read/write to read only, or reverse
 - Etc.
- System Hardware Actions
 - Enable or disable a parallel port

- Enable or disable a serial port
- Enable or disable a USB port
- etc
- Application Actions
 - General:
 - Launch a named application
 - Uninstall a named application
 - etc.
 - Email:
 - Adjust bandwidth available to email application
 - Remove recipients from outbound emails
 - Discard email
 - etc.
 - Application transactions
 - Initiation or blocking of specific transaction types for named applications
- VPN Client Actions
 - Establish VPN tunnel
 - Disconnect VPN tunnel
 - Establish VPN tunnel to a specified VPN server
 - Update VPN profile
- Antivirus Agent Actions
 - Delete a malicious file
 - Quarantine or otherwise disable a malicious file
 - Quarantine or otherwise disable infected files
- Personal Firewall Agent Actions
 - Block outbound access from specific application(s)
 - Block outbound access to specific destination IP address(es)
 - Block outbound from specific communication protocols, e.g. TCP, HTTP, policy

management client-server protocol, etc.)

- etc.
- Content Filtering Agent Actions
 - Block outbound access to specific DNS hostnames (e.g. www.cnn.com,) or specific realm(s) (e.g. *.si.com)
- Spyware Management Agent Actions
 - Delete a malicious file
 - Quarantine or otherwise disable a malicious file
 - Prevent specific software from loading into memory
- File System Actions
 - Delete a named file
 - Set the attributes of a named file to read-only
 - Move a named file to a specified local or remote location
 - etc.
- Data Backup Actions
 - Initiate partial or full backup
 - Initiate a local or remote backup of selected files and/or folders.
 - Suspend a backup process
 - Restart/Resume a backup process
- Data Access Actions
 - Restrict access privileges to specific data sources
 - Block write access privileges to specific data sources
 - Restrict copy privileges for specific data sources
 - etc.
- Network Connectivity Actions
 - Permit or deny network connectivity on a named dial adapter
 - Permit or deny network connectivity on a named network adapter

- Change TCP window size to throttle bandwidth consumption for all applications, for selected applications, for all communication protocols, and/or for selected communications protocols, for traffic destined to a specific destination IP address or address range, etc.
- etc.
- Network Services Actions
 - Disable DNS
 - Add default DNS server to endpoint configuration settings
 - Add entry to hosts file
 - etc.
- Access Control List Actions
 - Permit or deny network access to an enumerated list of IP addresses or IP network numbers
 - Permit or deny network access to an enumerated list of TCP or UDP ports or port ranges
 - Permit or deny network access to an enumerated list of applications
- Alerting Actions
 - Sending an email alert to a named email address
 - Send an alert to the user interface so the user is aware of the endpoint's state
 - Send an alert to the user interface so the user is aware of the policy violations
 - etc.
- Logging Actions
 - Log the policy violation(s) detected on the local machine
 - Send a policy violation(s) log message to a remote machine
- User Actions, Applications, Results, Restrictions, etc. Dimension (the OUTPUT dimension)
 - Allow certain applications
 - Block VPN connectivity

- Execute remediate actions (could be nested depending upon issues remediated)
- etc.

[0247] As noted and described above, examples and illustrations throughout are illustrative and not limiting. Numerous others will occur to the reader.

[0248] Having analyzed conditions and compared existing conditions to required conditions as described in the policy data store 106B, the analysis engine 106C determines what actions to initiate (step 212). The analysis engine 106C and its operative models and algorithms provide the ability to proactively take an exhaustive and extensible list of permissive, corrective or restrictive actions. The actions can be taken immediately, scheduled to occur at some future point in time, upon completion of some predefined system event, or as a prerequisite to some predefined system event. The actions when taken can also be logged by the agent and made available to a central management reporting console. Also, the actions may result in notifications or alerts being displayed to the end user, and/or uploaded to a central management reporting console.

[0249] For example the analysis engine can initiate the following actions:

- User management:
 - Disable a login account
 - Automatically log a user out of an application, the system, a secure connection, etc.
 - Require an immediate password reset.
- Application management:
 - Launch a specified application
 - Tear down a specified application
 - Prevent a specified application from launching
 - etc.
- Operating system management
 - Reprioritize running processes and threads

- Network management:
 - Prevent network connectivity to a local network
 - Prevent network connectivity to a remote network
 - Prevent use of one or more network adapters
 - Etc.
- Personal firewall:
 - Modify access control policies being enforced by firewall
 - Update access control list
- VPN client:
 - Change tunnel state
 - Force profile
- Data management:
 - Restrict access privileges to specific data sources
 - Block write access privileges to specific data sources
 - Restrict copy privileges for specific data sources
 - etc.
- Application specific management:
 - Initiation or blocking of specific application transaction types
- IT notification:
 - upon a new, previously unknown event, send an alert to a mail server to notify IT admin describing the issue and providing 2 links, one for approve, one for deny. IT selects one, clicks link, and is taken to web page where he logs in and submits the policy definition.

With respect to actions that may be initiated regarding hardware remediation:

- Issue end point software and/or hardware information update to IT asset management system
- Issue repair request to IT computing hardware repair system
- Issue device theft/loss message to IT asset management tracking system
- etc.

Communication of Endpoint State Information, Endpoint Compliance Analysis Results
And/Or Compliance Actions to a Remote Computer

[0250] There are a number of alternative implementations for how the invention can be instantiated and operated. Several examples of implementation methods supported by the invention follow. This list is exemplary and not exhaustive; others will now be apparent to the reader.

Implementation Method 1 - Endpoint system 104 Only

[0251] In this implementation scenario, all components are deployed on the endpoint system 104 being managed. This implementation is representative of a consumer-type offering where the system owner, invention operator, system administrator and invention administrator roles are all performed by the same single person. In this implementation, the logical components of the invention might be distributed across different systems as follows:

- Endpoint system 104 components:
 - Endpoint state data collection of conditions
 - Endpoint state data analysis
 - Compliance analysis engine
 - Policy-based actions
 - Policy data store
 - Policy management functions
 - Reporting functions
 - (all as described above)
- Policy management system 106 components:
 - None
- Host system 102 components:
 - None

Implementation Method 2 – Centralized endpoint system policy management

[0252] In this implementation, a central management user interface 106A on the policy management system 106 is used to configure policies that are then saved to a central policy data store 106B. The policies are synchronized or replicated to local policy databases residing in the endpoint system 104, for example in data store 104B, on a periodic basis when the endpoint system 104 checks in with the policy management system 106 to see if updates are available. An analysis engine, performing generally the same functions as engine 106C, residing on the endpoint system 104 is responsible for enforcing all compliance policies on the endpoint system 104 in accordance with policies received from the policy management system 106. This implementation is representative of a corporate-type offering or a managed services-type offering as might be provided by a service provider firm, where the endpoint system user is different from the endpoint system administrator or invention administrator roles. In this implementation, an exemplary distribution of invention components across different systems is as follows:

- Endpoint system 104 components:
 - Endpoint state data collection of conditions
 - Endpoint state data analysis
 - Compliance analysis engine
 - Policy-based actions
 - Policy data store
 - Policy management console
 - Reporting console
 - (all as described above)
- Policy management system 106 components:
 - Policy data store
 - Policy management functions
 - Reporting functions
- Host system 102 components:
 - None

[0253] In this implementation, conditions information, compliance violations and policy enforcement actions can be logged locally on the endpoint system 104 and/or

uploaded to any remote computer over a data communications network for centralized management reporting purposes. Data received from multiple endpoint systems 104 can also be aggregated for additional management reports. Information logged locally on the endpoint system 104 can also be viewed locally on the endpoint system by an operator of that system.

Implementation Method 3 – Centralized host system policy management

[0254] In this implementation scenario, a central management user interface 106A on the policy management system 106 is used to configure policies that are then saved to a central policy data store 106B. The policies are synchronized or replicated to a local policy database residing on the host system 102, for example in data store 102B, on a periodic basis when the host system 102 checks in with the policy management system 106 to see if updates are available. An analysis engine residing on the host system 102, performing generally the same functions as described with respect to engine 106B, is responsible for enforcing all compliance policies on the host system 102 in accordance with policies received from the policy management system 106. This implementation is representative of a client-server type application environment where client applications (e.g. web browser, database client, etc.) residing on endpoint systems 104 initiate communication sessions with server applications (e.g. web server, database management system, etc.) residing on host system 102 to upload and/or download application-specific data. In this type of client-server environment, it is important to ensure the host system 102 is protected at all times so that the host system 102 can not be compromised by a rogue endpoint system 104, or so that the host system 102 is prevented from sending malicious data or software code to endpoint system 104. In this implementation, an exemplary distribution of invention components across different systems is as follows:

- Endpoint system 104 components:
 - None
- Policy management system 106 components:
 - Policy data store
 - Policy management functions
 - Reporting functions

- Host system 102 components:
 - Endpoint state data collection of conditions
 - Endpoint state data analysis
 - Compliance analysis engine
 - Policy-based actions
 - Policy data store
 - Policy management functions
 - Reporting functions
 - (all as described above)

[0255] In this implementation, conditions information, compliance violations and policy enforcement actions can be logged locally on the host system 102 and/or uploaded to any remote computer over a data communications network for centralized management reporting purposes. Data received from multiple host systems 102 can also be aggregated for additional management reports. Information logged locally on the host system 102 can also be viewed locally on the endpoint system by an operator of that system.

Implementation Method 4 – Centralized analysis engine and compliance analysis of individual systems

[0256] In this implementation scenario, a policy management system 106 is used to configure compliance policies that are then saved to a policy data store 106B. Policies are also defined that identify what conditions 104F should be monitored by the agent monitoring components 104D, E residing on endpoint system 104 and/or host system 102. These policies are also stored in the policy data store 106B. Monitoring policies are subsequently distributed to endpoint system 104 and/or host system 102 periodically. An agent monitoring module residing on the endpoint system 104, performing generally this same functions as described with respect to engine 106B, collects endpoint condition information 104F and transmits it to the policy management system 106 where compliance analysis is performed using an analysis engine 106C. The analysis engine residing on the endpoint system (or equally the analysis engine residing on the host

system 102) does not perform compliance analysis. The analysis engine 106B in the policy management system 106 decides what policy enforcement actions are necessary. The policy enforcement decisions are sent from the policy management system 106 to the endpoint system 104 or the host system 104 as appropriate where the local system executes the policy enforcement actions as instructed by the policy management system 106. In this implementation, an exemplary distribution of invention components across different systems is as follows:

- Endpoint system 104 components:
 - Endpoint state data collection of conditions
 - Policy-based actions
- Policy management system 106 components:
 - Policy data store
 - Policy management functions
 - Reporting functions
 - Compliance analysis engine
 - Identification of policy-based actions to take
- Host system 102 components:
 - Endpoint state data collection of conditions
 - Policy-based actions

Implementation Method 5 – Centralized analysis engine and compliance analysis of multiple systems

[0257] In this implementation scenario, a policy management system 106 is used to configure compliance policies that are then saved to a policy data store 106B. The policy management system 106 can create one set of compliance policies it uses locally in its own analysis engine 106B and one or more sets of compliance policies it distributes to endpoint systems. Different sets of compliance policies may have the same or different values regarding items monitored, compliance thresholds, analysis methods to use, etc. Policies are also defined that identify what conditions 104F should be monitored by the agent monitoring components 104C, D residing on endpoint system 104 and/or host system 102. These policies are also stored in the policy data store 106B. Monitoring

policies are subsequently distributed to endpoint system 104 and/or host system 102 periodically. An agent monitoring module residing on the endpoint system 104, performing generally the same functions as described with respect to engine 106C, collects endpoint condition information 104F and forwards the aggregate data set of endpoint condition information 104 to the local analysis engine residing on the endpoint system.

[0258] A host system 102 if similarly configured would behave in a similar way. Thus the analysis engine local to the endpoint system collects endpoint state data, performs local compliance analysis and makes local policy action decisions. In addition to the local system (endpoint system 104 and/or host system 102) analyzing the condition information, the local system uploads the information to the policy management system 106. The analysis engine 106C residing in the policy management system 106 examines the aggregated set of condition information across multiple or all endpoint systems simultaneously using one or more analytical methods previously described herein, e.g. a statistical analysis method, in order to look for trends across the endpoint population and to assess the overall level of compliance across the entire endpoint system population or across a specific endpoint system population sample, and will reach compliance decisions that are independent of and indeed may be different from compliance decisions made on endpoint systems due to different policy values used by the endpoint analysis engine and the policy management system analysis engine. The policy management system 106 will subsequently identify one or more policy enforcement actions that need to be taken, identify specific endpoint systems 104, 102 on which those actions need to be taken and send messages to the appropriate endpoint systems containing policy enforcement instructions. The policy management system will also send one or more policy enforcement action instructions to network access control devices such as VPN gateway, router, switch, remote access server, etc.

[0259] In this implementation, an exemplary distribution of invention components across different systems is as follows:

- o Endpoint system 104 components:
 - o Endpoint state data collection of conditions

- Endpoint state data analysis
- Compliance analysis
- Policy-based actions
- Policy data store
- Policy management functions
- Reporting functions
- Policy management system 106 components:
 - Policy data store
 - Policy management functions
 - Reporting functions
 - Endpoint state data collection of conditions
 - Endpoint state data analysis
 - Compliance analysis engine
 - Identification of policy-based actions to take and identification of specific endpoint and/or host systems that should take those actions.
- Host system 102 components:
 - Endpoint state data collection of conditions
 - Endpoint state data analysis
 - Compliance analysis
 - Policy-based actions
 - Policy data store
 - Policy management functions
 - Reporting functions

Implementation Method 6 – Policy management system as in-band access control mechanism

[0260] In this implementation scenario, a policy management system 106 is used to configure compliance policies that are then saved to a policy data store 106B. Policies identify what conditions 104F should be monitored by the agent monitoring components 104C, D residing on endpoint system 104 and/or host system 102. The policy management system is integrated with a network access control function such that user or

application data exchanged between endpoint system 104 and host system 102 must pass through the combined policy management system/network access control function.

When the endpoint system 104 tries to access the host system 102, the access control function challenges the endpoint system 104 to provide condition information (i.e. inputs to the endpoint analysis engine) and/or compliance evaluation results (i.e. outputs from the endpoint analysis engine). When the endpoint system 104 returns the requested information, the access control function relays the information to the policy management system 106.

[0261] The policy management system 106 evaluates the compliance state of the endpoint system 104 based on information provided by the endpoint system 104 and policy data residing in the policy management system policy data store 106B. The policy management system 106 then makes one or more access control decisions. Access decisions might result result in unrestricted access, total denial of access or partially restricted access (e.g. specific destination IP addresses, address ranges, applications, protocols, etc.) to network resources such as applications residing on host system 102. The access control decisions made by the policy management system 106 are passed to the access control function. The access control function then automatically configures one or more access control rules for that endpoint system 104. Thereafter all endpoint system 104 data traffic sent through the access control function is either permitted or blocked in accordance with those access control rules. The access control function periodically issues challenges to the endpoint system 104 over the life of a communications session. The challenge requires the endpoint system 104 to re-submit compliance information in order to be permitted to maintain an active session with the network access function.

[0262] As the policy management system functionality and the access control function are two separate functions, they can be installed together on a shared computing device or alternatively can be installed separately on two different computing devices interconnected by a data communications network.

[0263] It will be obvious that the several methods just described are complementary. As such, various combinations of these methods are possible and are within the scope of this invention.

Data Sharing

[0264] The raw condition information collected by the agent monitor 104C, the compliance analysis conclusions reached by the analysis engine 106C, and/or compliance actions identified as necessary by the analysis engine 106C is available to external security-centric or other software agents running on the same system via the invention's API. The information is also available to remote systems via data communications networks and traditional client-server communication protocols (e.g. HTTP) or peer-to-peer communications protocols. This allows information collected or conclusions created by the invention to be utilized by other software and network access agents as part of their host or network assessment process.

[0265] While the various endpoint, host and policy management systems are described as communicating directly with one – another, it will be understood that the invention is not thus limited. Numerous intermediary parties may be associated with the collection and forwarding of agent information from endpoint system 104 to policy management system 106. Further, numerous additional intermediary systems may be associated with communicating the policy assessment and action information from policy management system 106 to host system 102.

Remote Administrator Notification and Control

[0266] The analysis engine 106C can be configured via policy settings to send a message to an administrator via a conventional data communications network and a commonly available data communications protocol, (e.g. via POP, SMTP, FTP, HTTP, etc.) when a specific policy event occurs, for example a specific noncompliance condition. Additionally, messages can be sent to an administrator when an unrecognized event occurs. In one embodiment, a message could be sent from the client to a policy-defined server using email or any other communication method. The server would in term

create or forward an email message to a policy defined email address. The email can contain a description of the event and 2 links: One to approve the action and one to deny the action. Clicking on the link would causes the IT administrator's web browser to open and send an HTTP request to the policy management server. There the IT administrator can be authenticated and prompted to confirm his intent and desires on the particular policy question. When the IT administrator successfully authenticates and submits the transaction, the policy setting is updated on the server policy data store. The next time the client (or any client in the same policy group) checks in with the server, it will automatically retrieve and apply the updated policy. Other embodiments for sending policy event notifications to an administrator are also possible and are within the scope of this invention.

[0267] There have thus been provided new and improved methods and systems for securing access to electronic resources, for example remote access to a host system and resources. The present invention applies one or more compliance assessment algorithms to collected system conditions, comparing the results to a security policy to determine if the system is in compliance with a security policy. One or more actions may be taken responsively. The present invention can use one or more of a variety of algorithms to assess large numbers of state conditions, making decisions based upon an essentially infinitely flexible security policy. The invention has commercial application in the field of electronic resource security.

[0268] Advantages of the invention include, without limitation:

- Heightened awareness and dynamic, autonomous adjustment to alert and enforcement thresholds based on condition data.
- Having a host system self-modulate what local resources are allowed to be accessed by remote systems based on its own self-assessment of conditions
- Having a policy management system alert a host system regarding conditions on the network as a whole (i.e. a plurality of end points) or specific end points and either A) explicitly instruct the host system regarding what local resources can be accessed by remote systems, or B) alert the host of conditions such that the host is

able to incorporate this data into its own self assessment and subsequently self-modulate what local resources are allowed to be accessed by remote systems based on its own self-assessment of conditions

- The use of industry standard vulnerability scores or risk indexes associated with published vulnerabilities, i.e. para 0053 and subsequent
- The conversion of non-quantitative end point state info, or conditions into quantitative values
- The use of quantitative analysis models in end point inspection, analysis and policy enforcement
- Extensibility to support different and future quant models
- Simultaneous and concurrent use of different analysis models, both quant and non quant to inspect different aspects of the end point
- Granular inspections and a wide multitude of conditions data collected) in order to assess the end point state from a more holistic level
- Granular and wide ranging policy enforcement capabilities, i.e. ability to influence a number of agents and conditions simultaneously
- Specific use of the quant models defined herein
- Extensibility of condition inspection capabilities
- Extensibility of agents integrated with
- Extensibility of compliance policies
- Extensibility of policy enforcement actions
- Ability to define compliance policies in terms of logical combinations of conditions

- Ability to define compliance policies in terms of quantitative terms
- Ability to define compliance policies for non quant conditions in quant terms
- Ability to combine analysis methods and create N-stage analysis sequences
- the notion of graduated levels of compliance and graduated levels of local permissions/restrictions depending on your level of compliance

[0269] While the invention has been shown and described with respect to particular embodiments, it is not thus limited. Numerous modifications, changes, enhancements and improvements within the scope of the invention will now be apparent to the reader.

WHAT IS CLAIMED IS:

1. A method operable on a computer for controlling the operation of a computing system in response to a security vulnerability, comprising:
 - the computing system running software subject to at least one security vulnerability;
 - establishing a policy based on the status of the at least one security vulnerability including at least one rule and an analysis method for determining compliance with the rule;
 - receiving information relating to the status of the at least one security vulnerability of the software program;
 - processing the information relating to the status using the analysis method;
 - determining, based on the processing, the compliance of the at least one security vulnerability in relation to the rule; and
 - controlling, based on the determining, the operation of the computing system.
2. The method of claim 1 wherein the software is a commercial product and the information relating to the status of the at least one known security vulnerability is made available to users of the software.
3. The method of claim 2 wherein the step of receiving information includes the steps of:
 - identifying a remote data repository wherein the information relating to the status of the at least one security vulnerability is available;
 - periodically checking the remote data repository to determine the availability of the information relating to the status; and
 - retrieving the information relating to the status.
4. The method of claim 3 wherein the step of receiving information further includes the step of storing locally the information relating to the status.

5. The method of claim 4 wherein the information relating to the status is selected from the group including a quantitative value and a non-quantitative value.
6. The method of claim 5 and further including the step of, prior to the processing, converting a non-quantitative value to a quantitative value.
7. The method of claim 6 wherein the analysis method is a quantitative analysis method.
8. The method of claim 1 wherein the step of controlling includes the step of taking a first action to negate the security vulnerability.
9. The method of claim 8 further including the steps of:
determining if the first action to negate the security vulnerability was successful;
and
taking, if the first action to negate the security vulnerability was not successful, a second action to diminish the threat of the security vulnerability.
10. The method of claim 9 wherein the second action is selected from a list comprising restricting access to a resource accessible using the computing system, automatically initiating an update to the software and automatically notifying an operator of the computing system.
11. The method of claim 1 and further including the steps of:
identifying within the computing system a plurality of conditions, each condition having a state; and
the policy further based upon the state of the conditions.
12. The method of claim 11 wherein at least one condition state is a quantitative value and at least one condition state is a non-quantitative value and wherein the analysis

method includes the combination of a quantitative analysis method and a non-quantitative analysis method.

13. The method of claim 11 wherein the step of identifying includes using a software agent.

14. The method of claim 13 wherein the step of controlling includes transmitting to the software agent an instruction to take an action.

15. The method of claim 1 wherein the computing system comprises at least one of a host computing system including a computing resource and an end point computing system pursuing access to the resource of the host computing system.

16. The method of claim 15 wherein the steps of establishing, receiving, processing, determining, and controlling are performed on at least one of the group comprising the computing system, the endpoint computing system and a policy management system connected to at least one of the computing system and the endpoint computing system.

17. A system for controlling the operation of a computing system in response to a security vulnerability, comprising:

- a processor;

- a memory connected to the processor and storing instructions for controlling the operation of the processor to perform the steps of

- identifying the computing system running software subject to at least one security vulnerability;

- storing a policy based on the status of the at least one security vulnerability including at least one rule and an analysis method for determining compliance with the rule;

- receiving information relating to the status of the at least one known security vulnerability of the software program;

- processing the information relating to the status using the analysis method;

determining, based on the processing, the compliance of the at least one security vulnerability in relation to the rule; and
controlling, based on the determining, the operation of the host computing system.

17. A method operable on a computer for controlling the access of an endpoint computing system to a host computing system in response to a security vulnerability, comprising:

identifying within at least one of the endpoint and host systems a plurality of conditions, each condition having a state;
operating on at least one of the host computing system and the endpoint computing system a software program subject to at least one security vulnerability;
establishing a policy based on the status of the at least one security vulnerability and the state of each of the plurality of conditions, the policy including at least one rule and an analysis method for determining compliance with the rule;
receiving information relating to the status of the at least one known security vulnerability of the software program;
receiving information relating to the state of each of the plurality of conditions;
processing the information relating to the status of the at least one known security vulnerability and the state of each of the plurality of conditions using the analysis method;
determining, based on the processing, the compliance of the at least one security vulnerability and the plurality of conditions with the rule; and
controlling, based on the determining, access of the endpoint system to a resource of the host computing system.

18. The method of claim 17 wherein the step of receiving information relating to the status of the security vulnerability includes the steps of:
identifying a remote data repository wherein the information relating to the status of the at least one known security vulnerability is available;

periodically checking the remote data repository to determine the availability of the information relating to the status; and
retrieving the information relating to the status.

19. The method of claim 18 wherein the step of receiving information further includes the step of storing locally the information relating to the status.

20. The method of claim 17 wherein the step of receiving information relating to the state of each of the plurality of conditions includes using a plurality of software agents to collect state information and at least one manager to aggregate the state information collected by the software agents.

21. A system for controlling the access of an endpoint computing system to a host computing system in response to a security vulnerability, comprising:
means for identifying within at least one of the endpoint and host systems a plurality of conditions, each condition having a state;
means for operating on at least one of the host computing system and the endpoint computing system a software program subject to at least one security vulnerability;
means for establishing a policy based on the status of the at least one security vulnerability and the state of each of the plurality of conditions, the policy including at least one rule and an analysis method for determining compliance with the rule;
means for receiving information relating to the status of the at least one known security vulnerability of the software program;
means for receiving information relating to the state of each of the plurality of conditions;
means for processing the information relating to the status of the at least one known security vulnerability and the state of each of the plurality of conditions using the analysis method;
means for determining, based on the processing, the compliance of the at least one security vulnerability and the plurality of conditions with the rule; and

means for controlling, based on the determining, access of the endpoint system to a resource of the host computing system.

22. A method for generating signals to control the access of an endpoint computing system to a resource in a host computing system, comprising:

collecting a state for each of a plurality of conditions in at least one of the endpoint computing system and the host computing system;

collecting a status of a known security vulnerability for a software program operating on at least one of the host computing system and the endpoint computing system;

identifying a policy for determining access of the endpoint computing system to the resource, the policy including at least one rule and an analysis method for determining compliance with the rule;

processing, using the analysis method, the state of each of the plurality of conditions and the status of the known security vulnerability;

determining, based upon the processing, if the conditions and the known security vulnerability are in compliance with the rule; and

generating, based upon the determining, a signal usable to control the access of the endpoint computing system to the resource.

23. The method of claim 22 wherein the endpoint computing system is selected from the group including a user of the host computing system and an endpoint computing system separate from the host system.

24. A program product containing instructions to control the operation of a computing system to control the access of an endpoint computing system to a resource in a host computing system, the instructions operable on the computing system to cause the computing system to perform a process comprising:

collecting a state for each of a plurality of conditions in at least one of the endpoint computing system and the host computing system;

collecting a status of a known security vulnerability for a software program operating on at least one of the host computing system and the endpoint computing system;

identifying a policy for determining access of the endpoint computing system to the resource, the policy including at least one rule and an analysis method for determining compliance with the rule;

processing, using the analysis method, the state of each of the plurality of conditions and the status of the known security vulnerability;

determining, based upon the processing, if the conditions and the known security vulnerability are in compliance with the rule; and

generating, based upon the determining, a signal usable to control the access of the endpoint computing system to the resource.

25. A method for developing a compliance policy to control the access of an endpoint computing system to a resource in a host computing system, comprising:

identifying a plurality of conditions in at least one of the endpoint computing system and the host computing system, each of the plurality of conditions including an associated state, at least one of the plurality of conditions relating to a risk of a known security vulnerability; and

developing a policy for determining the access of the endpoint computing system to the resource, the policy including a rule and at least one analysis method for processing the states of the plurality of conditions to determine if the plurality of conditions are in compliance with the rule.

27. The method of claim 25 wherein the at least one condition relating to a risk of a known security vulnerability includes a state determined at least in part by security risk information provided by a third-party.

28. A system for developing a compliance policy to control the access of an endpoint computing system to a resource in a host computing system, comprising:

means for identifying a plurality of conditions in at least one of the endpoint computing system and the host computing system, each of the plurality of conditions including an associated state, at least one of the plurality of conditions relating to a risk of a known security vulnerability; and

means for developing a policy for determining the access of the endpoint computing system to the resource, the policy including a rule and at least one analysis method for processing the states of the plurality of conditions to determine if the plurality of conditions are in compliance with the rule.

Methods and Systems for Controlling Access to Computing Resources Based on Known
Security Vulnerabilities

Abstract Of The Invention

Methods and systems are provided for fine tuning access control by remote, endpoint systems to host systems. Multiple conditions/states of one or both of the endpoint and host systems are monitored, collected and fed to an analysis engine. Using one or more of many different flexible, adaptable models and algorithms, an analysis engine analyzes the status of the conditions and makes decisions in accordance with pre-established policies and rules regarding the security of the endpoint and host system. Based upon the conditions, the policies, and the analytical results, actions are initiated regarding security and access matters. In one described embodiment of the invention, the monitored conditions include software vulnerabilities.

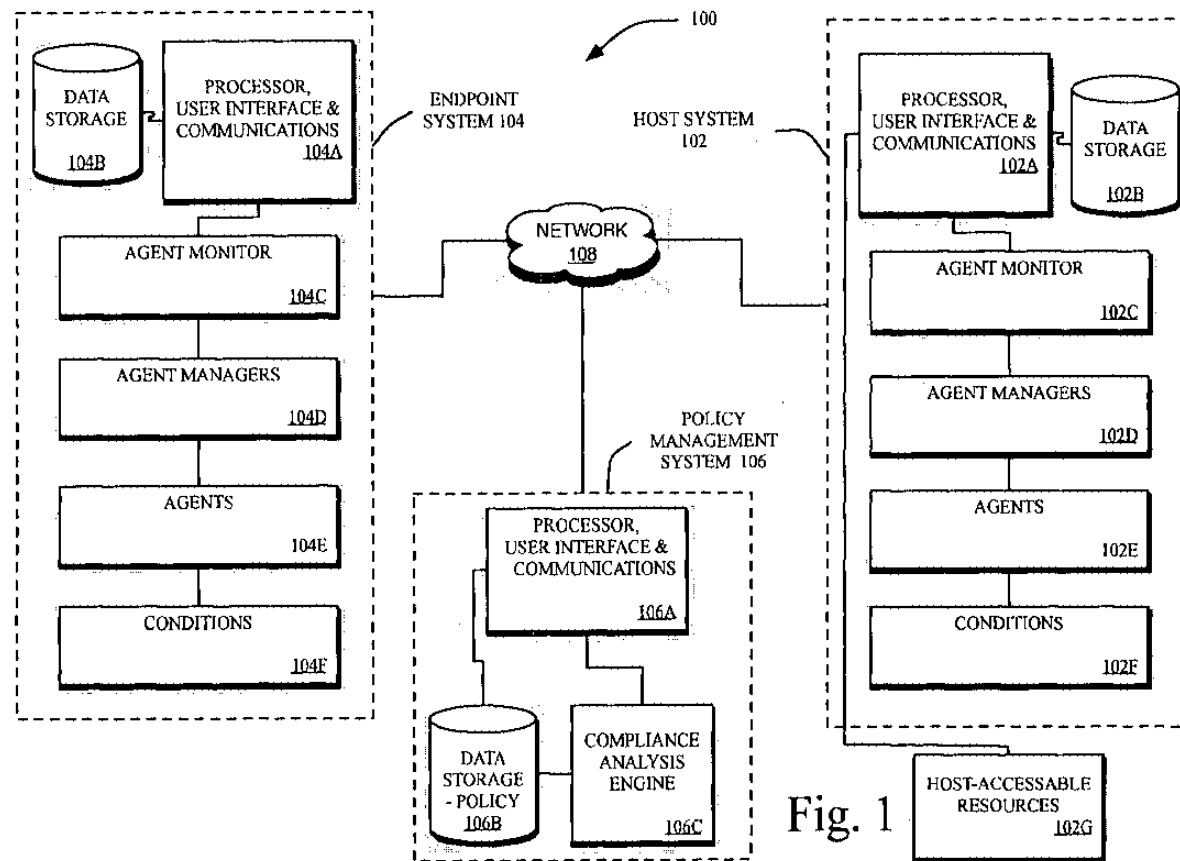


Fig. 1

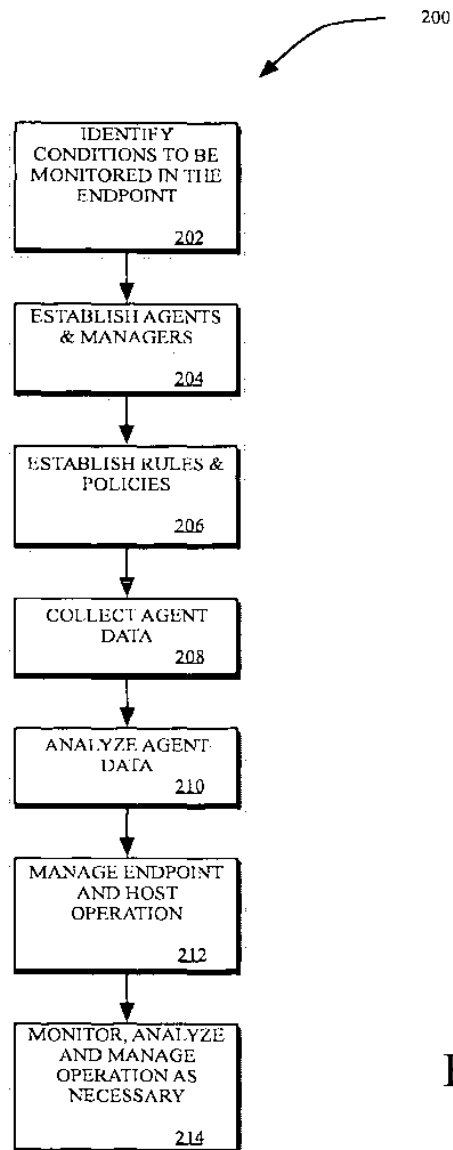


Fig. 2

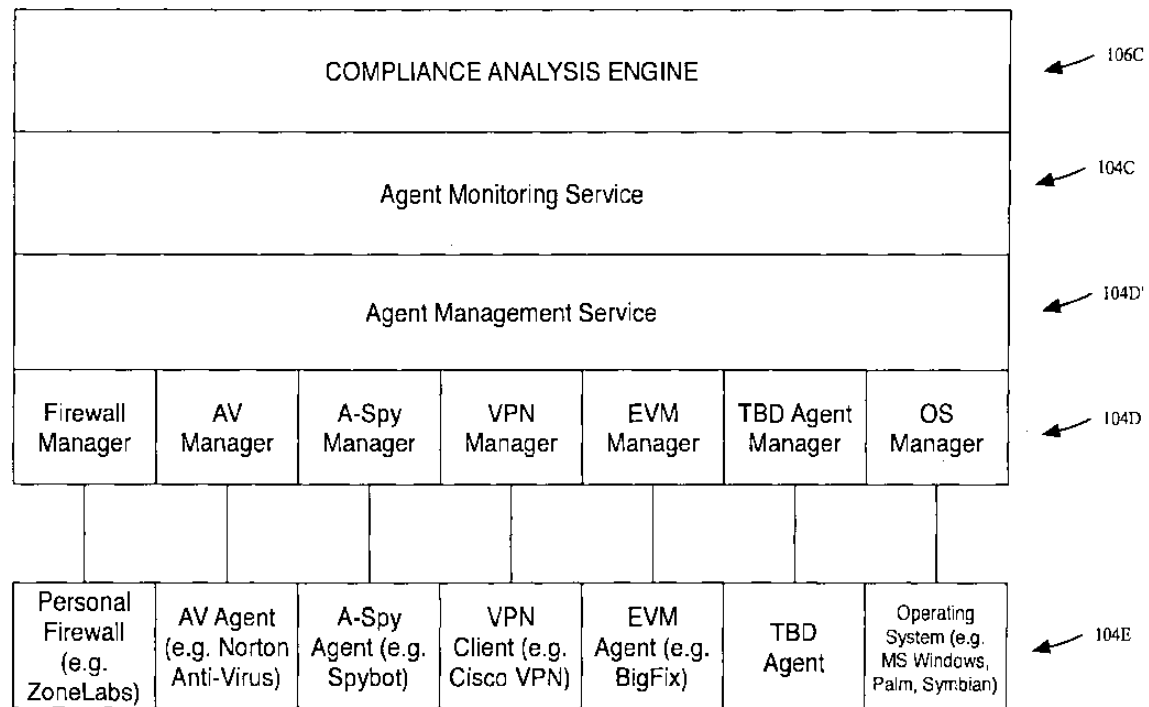


Fig. 3

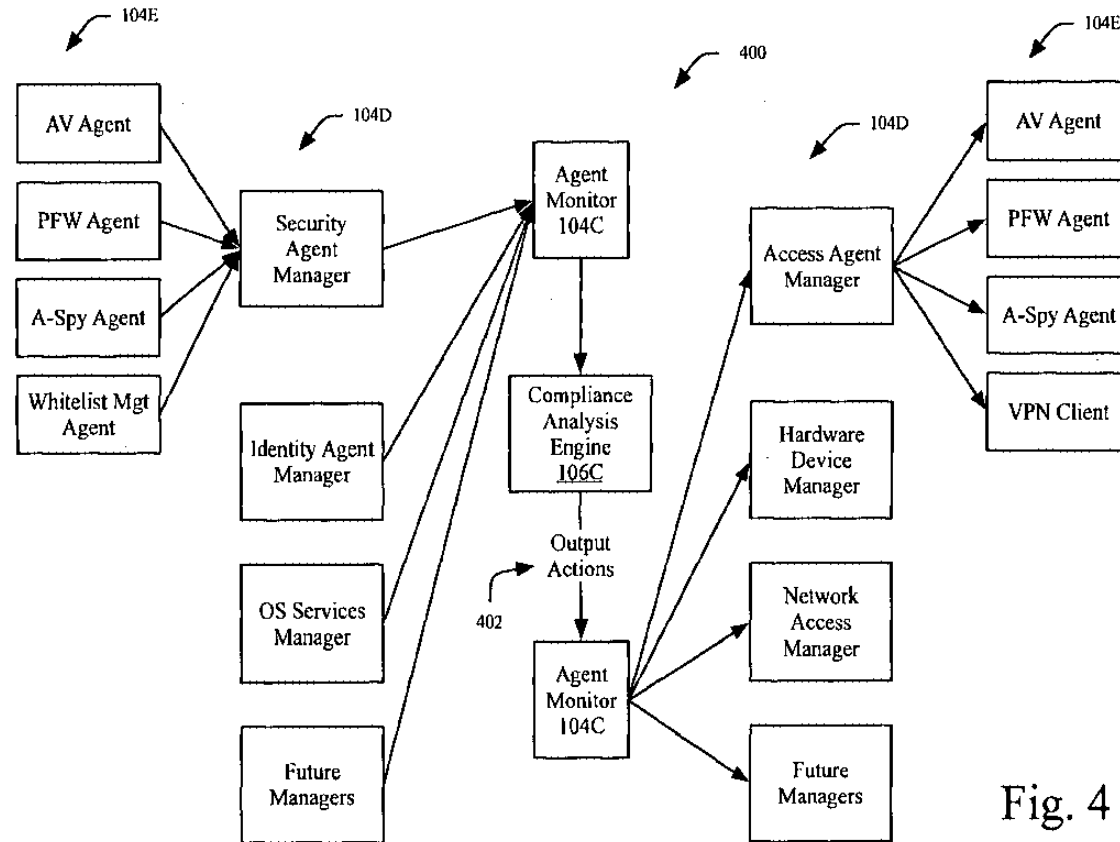


Fig. 4

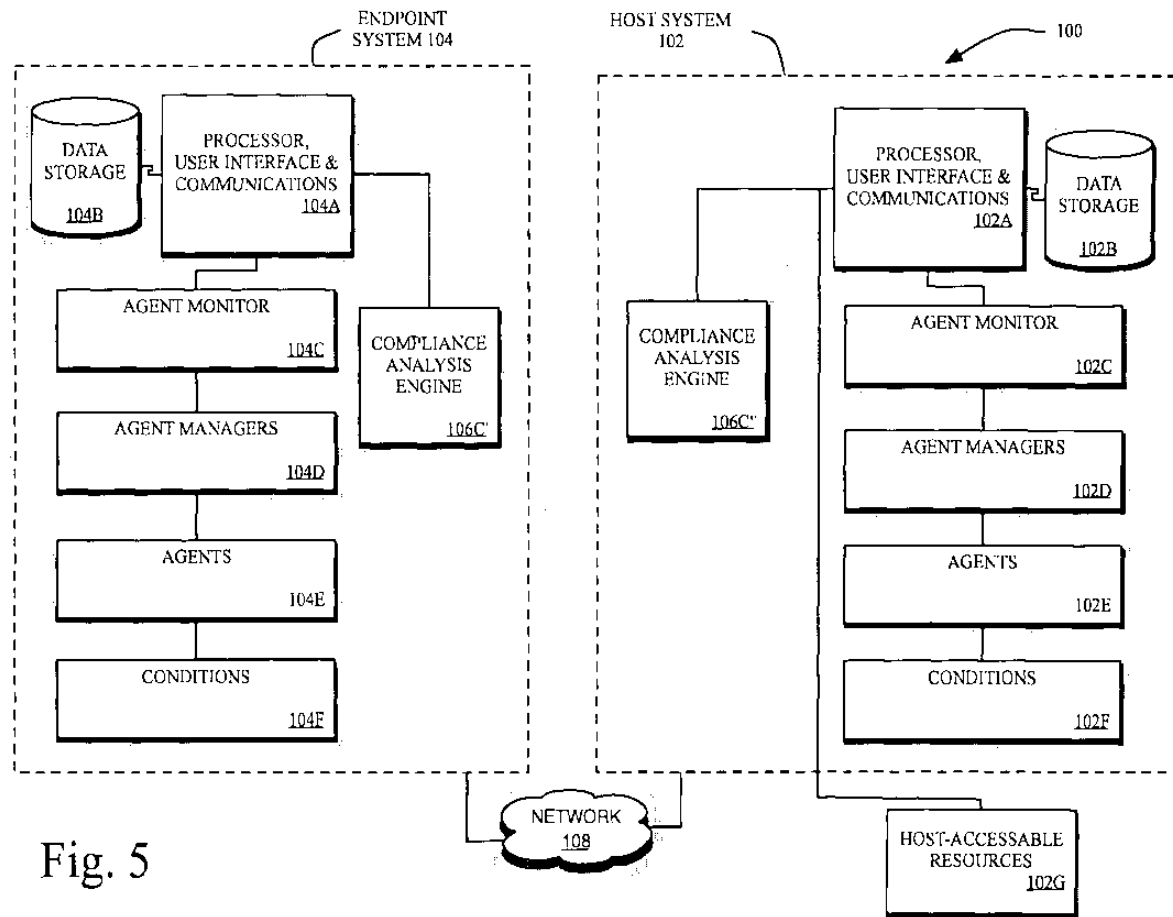


Fig. 5

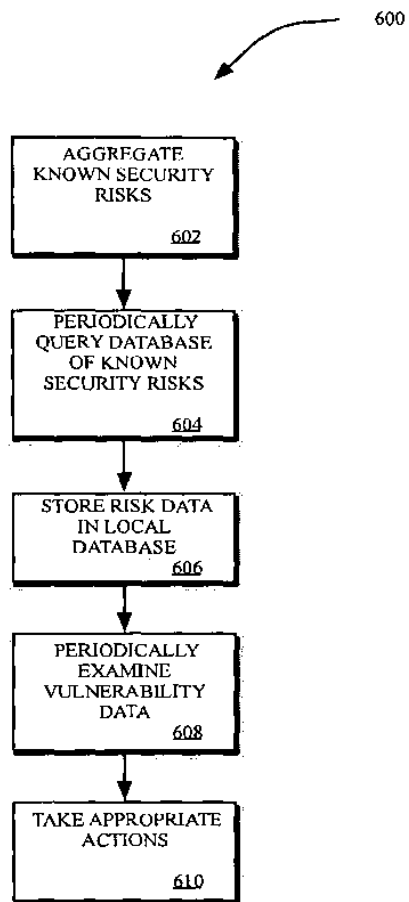


Fig. 6

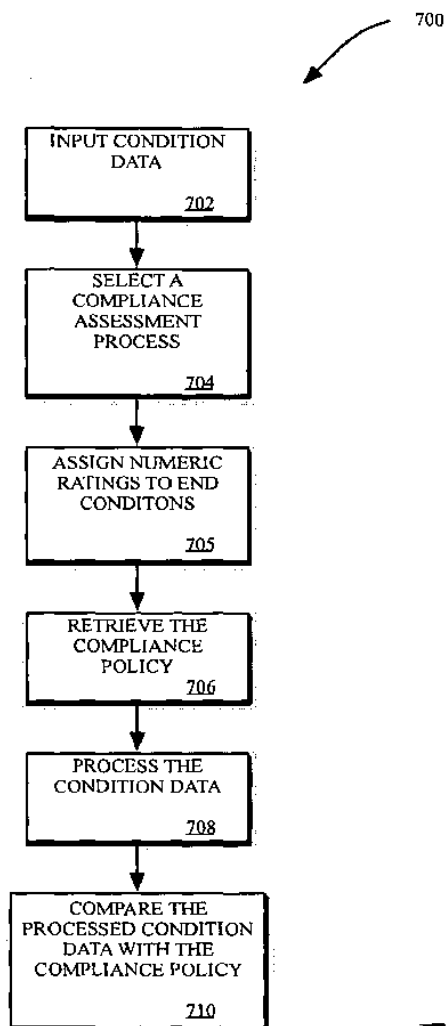


Fig. 7

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES.**

The specification of which is attached hereto.

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

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 C.F.R. § 1.56 (attached hereto). I also acknowledge my duty to disclose all information known to be material to patentability which became available between a filing date of a prior application and the national or PCT international filing date in the event this is a Continuation-In-Part application in accordance with 37 C.F.R. § 1.63(e).

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

No such claim for priority is being made at this time.

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

Application Number
60/752,424

Filing Date
December 21, 2005

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

No such claim for priority is being made at this time.

I hereby appoint the following attorney(s) and/or patent agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

Best Available Copy

Continuation Application
of Serial No. 11/451,950
Attorney Docket No. 130839.00921
Application No. Herewith
Customer No. 86308

Attorney Docket No.: 1291U004USD1
Serial No. not assigned
Filing Date: herewith

Page 2 of 3

CUSTOMER NUMBER: 33893

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization/who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Jeffrey L. Brandt, to the contrary.

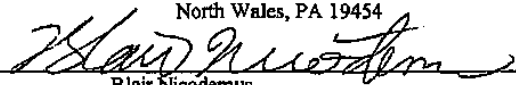
Please direct all correspondence in this case to Jeffrey L. Brandt at the address indicated below:

c/o Intellevate
P.O. Box 52050
Minneapolis, MN 55402
Telephone No. 203-438-1077

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

Full Name of joint inventor number 1: Blair Nicodemus
Citizenship: United States of America
Post Office Address: 143 Polo Drive
North Wales, PA 19454

Residence: North Wales, PA

Signature: 

Blair Nicodemus

Date: 5/6/2008

Full Name of joint inventor number 2: Billy Edison Stephens
Citizenship: United States of America
Post Office Address: 1104 Highgrove Drive
West Chester, PA 19380

Residence: West Chester, PA

Signature: _____

Billy Edison Stephens

Date: _____

Best Available Copy

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
- (2) It refutes, or is inconsistent with, a position the applicant takes in:
 - (i) Opposing an argument of unpatentability relied on by the Office, or
 - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
- (2) Each attorney or agent who prepares or prosecutes the application; and
- (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

Best Available Copy

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES.**

The specification of which is attached hereto.

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

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 C.F.R. § 1.56 (attached hereto). I also acknowledge my duty to disclose all information known to be material to patentability which became available between a filing date of a prior application and the national or PCT international filing date in the event this is a Continuation-In-Part application in accordance with 37 C.F.R. § 1.63(e).

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

No such claim for priority is being made at this time.

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

Application Number
60/752,424

Filing Date
December 21, 2005

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

No such claim for priority is being made at this time.

I hereby appoint the following attorney(s) and/or patent agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

Best Available Copy

Continuation Application
of Serial No. 11/451,950
Attorney Docket No. 130839.00921
Application No. Herewith
Customer No. 86308
Attorney Docket No.: 12910004USD1
Serial No. not assigned
Filing Date: herewith

Page 2 of 3

CUSTOMER NUMBER: 33893

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization/who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Jeffrey L. Brandt to the contrary.

Please direct all correspondence in this case to Jeffrey L. Brandt at the address indicated below:

c/o Intellevate
P.O. Box 52050
Minneapolis, MN 55402
Telephone No. 203-438-1077

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

Full Name of joint inventor number 1: Blair Nicodemus
Citizenship: United States of America
Post Office Address: 143 Polo Drive
North Wales, PA 19454

Residence: North Wales, CT

Signature: _____ Date: _____
Blair Nicodemus

Full Name of joint inventor number 2: Billy Edison Stephens
Citizenship: United States of America
Post Office Address: 1104 Highgrove Drive
West Chester, PA 19380

Residence: West Chester, PA

Signature: Billy Edison Stephens Date: 6/2/06
Billy Edison Stephens

Best Available Copy

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
- (2) It refutes, or is inconsistent with, a position the applicant takes in:
 - (i) Opposing an argument of unpatentability relied on by the Office, or
 - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
- (2) Each attorney or agent who prepares or prosecutes the application; and
- (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

Best Available Copy

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Dossier Number 13/587,505					
APPLICATION AS FILED - PART I											
(Column 1)		(Column 2)		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)			RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (d))	N/A	N/A	N/A	95			N/A				
SEARCH FEE (37 CFR 1.16(c), (d), or (f))	N/A	N/A	N/A	310			N/A				
EXAMINATION FEE (37 CFR 1.16(a), (d), or (h))	N/A	N/A	N/A	125			N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	28 minus 20 =	8	x 30	240	OR						
INDEPENDENT CLAIMS (37 CFR 1.16(i))	8 minus 3 =	5	x 125 =	625							
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	1395		TOTAL				
APPLICATION AS AMENDED - PART II											
AMENDMENT A	(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE(S)	ADDITIONAL FEE(S)		RATE(S)	ADDITIONAL FEE(S)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x			OR	x	
	Independent (37 CFR 1.16(i))	*	Minus	***	=	x	=		OR	x	=
	Application Size Fee (37 CFR 1.16(s))								OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								OR		
					TOTAL ADDL FEE			OR	TOTAL ADDL FEE		
AMENDMENT B	(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE(S)	ADDITIONAL FEE(S)		RATE(S)	ADDITIONAL FEE(S)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x			OR	x	=
	Independent (37 CFR 1.16(i))	*	Minus	***		x			OR	x	
	Application Size Fee (37 CFR 1.16(s))								OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								OR		
					TOTAL ADDL FEE			OR	TOTAL ADDL 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 figure 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: 400 M STREET, N.E., 5TH FLOOR
WASHINGTON, D.C. 20540
Alexandria, Virginia 22314-1150
www.uspto.gov

APPLICATION NUMBER	FILING DATE	GR PATENT UNIT	FEES RECEIVED	ATTY. DOK. KEY NO.	TOT. CLAIMS	IND. CLAIMS
13/587,505	08/16/2012	2431	0.00		28	8

CONFIRMATION NO. 9471

FILING RECEIPT



0000000056193623

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 08/30/2012

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

Applicant(s)

Blair Nicodemus, North Wales, PA;
Billy Edison Stephens, West Chester, PA;

Assignment For Published Patent Application

FIBERLINK COMMUNICATIONS CORPORATION, Blue Bell, PA

Power of Attorney: The patent practitioners associated with Customer Number 33893

Domestic Priority data as claimed by applicant

This application is a CON of 11/451,950 06/13/2006
which claims benefit of 60/752,424 12/21/2005

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

If Required, Foreign Filing License Granted: 08/27/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/587,505**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES
BASED ON KNOWN SECURITY VULNERABILITIES

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

page 2 of 3

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 Assets Control, 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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: 1500 M Street, NW, 4TH FLOOR
WASHINGTON, DC 20540
Alexandria, Virginia 22314-1150
www.uspto.gov

APPLICATION NUMBER	FILING OR PRIORITY DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./FILE NO.
13/587,505	08/16/2012	Blair Nicodemus	

CONFIRMATION NO. 9471

FORMALITIES LETTER



0000000056193624

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 08/30/2012

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

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

- The statutory basic filing fee is missing.
Applicant must submit \$95 to complete the basic filing fee for a small entity.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
 - The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) 1, 2, 5, 6, 7.

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.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **\$865** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of **\$65** for a small entity in compliance with 37 CFR 1.27, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is **\$1460** for a small entity

- **\$95** Statutory basic filing fee.
- **\$65** Surcharge.
- The application search fee has not been paid. Applicant must submit **\$310** to complete the search fee.
- The application examination fee has not been paid. Applicant must submit **\$125** to complete the examination fee for a small entity in compliance with 37 CFR 1.27.
- Total additional claim fee(s) for this application is **\$865**
 - **\$625** for **5** independent claims over 3.
 - **\$240** for **8** total claims over 20.

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.

<https://portal.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.

/hnguyen/

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

DOCKET NO.: 130839.00921

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Blair NICODEMUS et al.**

Title: **METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING
RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES**

Serial No.: **13/587505**

Group Art Unit: **2431**

Filed: **16 August 2012**

Examiner: **Not Yet Determined**

Confirmation: **9471**

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

VIA EFS
DATE SENT: March 29, 2013

Dear Sir:

PRELIMINARY AMENDMENT

Prior to examination on the merits, Applicants respectfully request that the application be amended as follows.

Amendment of the Claims begins at page 2.

Remarks begin at page 7.

This listing of claims will replace all prior versions, and listings of claims in the application.

Listing of Claims:

1-30. (Cancelled)

31. (new) A method for controlling the operation of an endpoint, comprising:
- providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;
 - maintaining the plurality of policies in a data store on the computing system;
 - identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor;
 - configuring one or more agents on the endpoint to monitor the plurality of conditions;
 - receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more agents;
 - determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and
 - initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store.
32. (new) The method of claim 31, wherein the action comprises controlling access of the endpoint to computing resources.
33. (new) The method of claim 31, wherein the user interface comprises a web page.
34. (new) The method of claim 31, further comprising requesting, at the computing system, the status information on a periodic basis.
35. (new) The method of claim 31, wherein the endpoint comprises a mobile device.

36. (new) The method of claim 31, wherein the plurality of agents comprise at least one service provided by the operating system of the endpoint.
37. (new) The method of claim 31, wherein the plurality of agents comprise at least one application running on the endpoint.
38. (new) The method of claim 31, wherein the conditions comprise at least one hardware condition.
39. (new) The method of claim 31, wherein the conditions comprise at least one software condition.
40. (new) The method of claim 31, wherein the computing system comprises a plurality of servers.
41. (new) The method of claim 31, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.
42. (new) A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising:
- providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;
 - maintaining the plurality of policies in a data store on the computing system;
 - identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor;
 - configuring one or more agents on the endpoint to monitor the plurality of conditions;
 - receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more agents;

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and

initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store.

43. (new) The computer readable medium of claim 42, wherein the action comprises controlling access of the endpoint to computing resources.
44. (new) The computer readable medium of claim 42, wherein the user interface comprises a web page.
45. (new) The computer readable medium of claim 42, further comprising requesting, at the computing system, the status information on a periodic basis.
46. (new) The computer readable medium of claim 42, wherein the endpoint comprises a mobile device.
47. (new) The computer readable medium of claim 42, wherein the plurality of agents comprise at least one service provided by the operating system of the endpoint.
48. (new) The computer readable medium of claim 42, wherein the plurality of agents comprise at least one application running on the endpoint.
49. (new) The computer readable medium of claim 42, wherein the conditions comprise at least one hardware condition.
50. (new) The computer readable medium of claim 42, wherein the conditions comprise at least one software condition.
51. (new) The computer readable medium of claim 42, wherein the computing system comprises a plurality of servers.

52. (new) The computer readable medium of claim 42, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.
53. (new) A system for controlling the operation of an endpoint, comprising:
- a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;
 - a data store, at the computing system, that contains the plurality of policies;
 - one or more agents on the endpoint configured to monitor a plurality of conditions identified in the plurality of policies; and
 - one or more processors at the computing system configured to:
 - receive, across a network, status information about the plurality of conditions on the endpoint gathered by the one or more agents,
 - determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and
 - initiate, based on the compliance state, an action identified in at least one rule in the data store.
54. (new) The system of claim 53, wherein the action comprises controlling access of the endpoint to computing resources.
55. (new) The system of claim 53, wherein the user interface comprises a web page.
56. (new) The system of claim 53, wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis.
57. (new) The system of claim 53, wherein the endpoint comprises a mobile device.

58. (new) The system of claim 53., wherein the plurality of agents comprise at least one service provided by the operating system of the endpoint.
59. (new) The system of claim 53, wherein the plurality of agents comprise at least one application running on the endpoint.
60. (new) The system of claim 53, wherein the conditions comprise at least one hardware condition.
61. (new) The system of claim 53, wherein the conditions comprise at least one software condition.
62. (new) The system of claim 53, wherein the computing system comprises a plurality of servers.
63. (new) The system of claim 53, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.

REMARKS

Claims 1-30 have been cancelled. New claims 31-63 have been added. Support for these claims can be found throughout the application. While many paragraphs support these claims, a non-exhaustive, illustrative list of paragraphs that may provide specific support for some or all of these new claims includes, but is not limited to the following paragraphs (as recited in the parent application publication): 15-19, 95-105, 106-114, 358-362, 613-615, 643-647, 730-731, 976-977, 1160-1203, and the accompanying figures and descriptions thereof. Many additional supportive examples are provided throughout the application. No new matter has been introduced.

CONCLUSION

Applicants respectfully submit that these new claims place this application in condition for allowance. The Examiner is invited to contact Applicants' undersigned representative if there are any questions regarding the captioned application.

Respectfully submitted,

by: /Michael K. Jones, Reg. No. 41,100/
Michael K. Jones
Registration No. 41,100

Dated: March 29, 2013
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Streets
Philadelphia, PA 19103-2799
(215) 981 - 4997 (Telephone)
(610) 640 - 7835 (Facsimile)

Electronic Patent Application Fee Transmittal				
Application Number:	13587505			
Filing Date:	16-Aug-2012			
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES			
First Named Inventor/Applicant Name:	Blair Nicodemus			
Filer:	Michael Kenneth Jones/Heather Busk			
Attorney Docket Number:				
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:				
Claims in excess of 20	2202	13	40	520
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 5 months with \$0 paid	2255	1	1500	1500
Miscellaneous:				
Total in USD (\$)				2820

Electronic Acknowledgement Receipt	
EFS ID:	15391619
Application Number:	13587505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair Nicodemus
Customer Number:	86308
Filer:	Michael Kenneth Jones/Heather Busk
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	
Receipt Date:	29-MAR-2013
Filing Date:	16-AUG-2012
Time Stamp:	16:10:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2820
RAM confirmation Number	2374
Deposit Account	500436
Authorized User	JONES, MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	Response.pdf	18904 63bce9c23e21c0e0c991f72b1c646419f895d	no	1
Warnings:					
Information:					
2	Extension of Time	921EOT.pdf	152038 6311d1110f7a8886c204761a29f439a741539	no	2
Warnings:					
Information:					
3	Preliminary Amendment	PRLAMD.pdf	41823 8bae4f958c9a2e5a1a295a8de11e01c5a1b5c49	no	7
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	40475 49229cc07c6c040c06cc088ba9f979a3300c	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			253240		
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>					

DOCKET NO. 130839.00921

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Blair NICODEMUS et al.**

**Title: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO
COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES**

Application No.: **13/587,505**

Group Art Unit: **2431**

Filed: **August 16, 2012**

Examiner: **To Be Determined**

Confirmation: **9471**

Filed by EFS on: **March 29, 2013**

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

Sir:

**RESPONSE TO NOTICE TO FILE MISSING PARTS
OF NON-PROVISIONAL APPLICATION**

Responsive to the Notification dated August 30, 2012, enclosed is payment of the declaration surcharge in compliance with 37 C.F.R. § 1.16(f) along with payment of the basic filing fee, as set forth in 37 C.F.R. § 1.16(a)(1), search fee, as set forth in 37 C.F.R. § 1.16(k), and examination fee, as set forth in 37 C.F.R. § 1.16(o). Figures 1-7 from parent application no. 11/451,950 were accepted by the Examiner on 7/22/2009. The figures from parent application no. 11/451,950 were filed as continuation application no. 13/587,505 on August 16, 2012. Applicant believes the figures are in compliance with 37 C.F.R. § 1.84 (b).

The Commission for Patents is hereby authorized to charge any deficiency or credit any overpayment to Deposit Account 50-0436.

Respectfully Submitted,

By: /Michael K. Jones, Reg. #41100/
Michael K. Jones
Registration No. 41,100

Dated: **March 29, 2013**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4405
Facsimile: (610) 640-7835

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 130839.00921
Application Number 13/587,505	Filed August 16, 2012	
For METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		
Art Unit 2431	Examiner To Be Determined	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application. The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):		
	<u>Fee</u>	<u>Small Entity Fee</u>
☐ One month (37 CFR 1.17(a)(1))	\$200	\$100
☐ Two months (37 CFR 1.17(a)(2))	\$600	\$300
☐ Three months (37 CFR 1.17(a)(3))	\$1,400	\$700
☐ Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100
☒ Five months (37 CFR 1.17(a)(5))	\$3,000	\$1,500
☒ Applicant asserts small entity status. See 37 CFR 1.27. ☐ Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously. ☐ A check in the amount of the fee is enclosed. ☒ Payment by credit card. Form PTO-2038 is attached. ☐ The Director has already been authorized to charge fees in this application to a Deposit Account. ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <u>50-0436</u> ☒ Payment made via EFS-Web.		
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. I am the <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div> ☐ applicant. ☒ attorney or agent of record. Registration number <u>41,100</u> ☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ </div> <div style="text-align: right;"> /Michael K. Jones, Reg. No. 41100/ Signature Michael K. Jones Typed or printed name </div> <div style="text-align: right;"> March 29, 2013 Date 215.981.4405 Telephone Number </div> </div>		
NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.		

☒ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop 1PC1, 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 disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Document Number 13/587,505		Filing Date 08/16/2012		☐ To be Valid	
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO									
APPLICATION AS FILED – PART I									
(Column 1)		(Column 2)							
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)	
☐ BASIC FEE (37 CFR 1.16(a)(1)(i)-(iv))		N/A		N/A		N/A			
☐ SEARCH FEE (37 CFR 1.16(a)(1)(v)-(vi))		N/A		N/A		N/A			
☐ EXAMINATION FEE (37 CFR 1.16(a)(1)(vii)-(viii))		N/A		N/A		N/A			
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =		^		X \$		-	
INDEPENDENT CLAIMS (37 CFR 1.16(j))		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									
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	03/29/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	+ 33	Minus	= 33	= 0	X \$40 =		0	
	Independent (37 CFR 1.16(j))	+ 3	Minus	= 3	= 0	X \$210 =		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			
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	=	Minus	=	=	X \$		-	
	Independent (37 CFR 1.16(j))	=	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.									

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-PATO-9199 and select option 2.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Dossier Number 13/587,505					
APPLICATION AS FILED - PART I											
(Column 1)		(Column 2)		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)			RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70			N/A				
SEARCH FEE (37 CFR 1.16(d), (e), or (f))	N/A	N/A	N/A	300			N/A				
EXAMINATION FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	360			N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	33	minus 20 =	13	x 40	520	OR					
INDEPENDENT CLAIMS (37 CFR 1.16(i))	3	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	1250		TOTAL				
APPLICATION AS AMENDED - PART II											
AMENDMENT A	(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE(S)	ADDITIONAL FEE(S)		RATE(S)	ADDITIONAL FEE(S)
	Total (37 CFR 1.16(i))	*	Minus	**		x			OR	x	
	Independent (37 CFR 1.16(i))	*	Minus	***	=	x	=		OR	x	=
	Application Size Fee (37 CFR 1.16(s))								OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								OR		
					TOTAL ADDL FEE			OR	TOTAL ADDL FEE		
AMENDMENT B	(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE(S)	ADDITIONAL FEE(S)		RATE(S)	ADDITIONAL FEE(S)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x			OR	x	=
	Independent (37 CFR 1.16(i))	*	Minus	***		x			OR	x	
	Application Size Fee (37 CFR 1.16(s))								OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								OR		
					TOTAL ADDL FEE			OR	TOTAL ADDL 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 figure 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: 1500 M Street, N.W., 4TH FLOOR
WASHINGTON, D.C. 20540
Alexandria, Virginia 22314-1150
www.uspto.gov

APPLICATION NUMBER	FILING OR EFFECT DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./FILE NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921

CONFIRMATION NO. 9471

WITHDRAWAL NOTICE



00000000060274546

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 04/10/2013

Letter Regarding a New Notice and/or the Status of the Application

If a new notice or Filing Receipt is enclosed, applicant may disregard the previous notice mailed on 08/30/2012. The time period for reply runs from the mail date of the new notice. Within the time period for reply, applicant is required to file a reply in compliance with the requirements set forth in the new notice to avoid abandonment of the application.

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://portal.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 the reply is not filed electronically via EFS-Web, the reply must be accompanied by a copy of the new notice.

If the Office previously granted a petition to withdraw the holding of abandonment or a petition to revive under 37 CFR 1.137, the status of the application has been returned to pending status.

/afeschaye/

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



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: 1000 M Street, NE, 8th Floor
Washington, DC 20536
Alexandria, Virginia 22314-1150
www.uspto.gov

APPLICATION NUMBER	FILING OR PRIORITY DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./FILE NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921

CONFIRMATION NO. 9471

FORMALITIES LETTER



0000000060274550

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 04/10/2013

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:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
 - The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) 1, 2, 5, 6, 7.

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.
<https://portal.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.

/afeschaye/

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



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: 1500 M Street, NW, 4th Floor
Washington, DC 20540
Alexandria, Virginia 22304-1150
www.uspto.gov

APPLICATION NUMBER	FILING DATE	CLASS CODE	CLASS SUBCLASS	ATTY. DOK. KEY NO.	TOTAL CLAIMS	IND. CLAIMS
13/587,505	08/16/2012	2431	1320	130839.00921	33	3

CONFIRMATION NO. 9471

FILING RECEIPT



OC00000060274549

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 04/10/2013

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)

Blair Nicodemus, North Wales, PA;
Billy Edison Stephens, West Chester, PA;

Applicant(s)

Blair Nicodemus, North Wales, PA;
Billy Edison Stephens, West Chester, PA;

Assignment For Published Patent Application

FIBERLINK COMMUNICATIONS CORPORATION, Blue Bell, PA

Power of Attorney: The patent practitioners associated with Customer Number 33893

Domestic Priority data as claimed by applicant

This application is a CON of 11/451,950 06/13/2006 ABN
which claims benefit of 60/752,424 12/21/2005

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: 08/27/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/587,505**

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

Non-Publication Request: No

Early Publication Request: No

page 1 of 3

**** SMALL ENTITY ****

Title

METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES
BASED ON KNOWN SECURITY VULNERABILITIES

Preliminary Class

726

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Document Number 13/587,505		Filing Date 08/16/2012		☐ To be Valid	
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO									
APPLICATION AS FILED – PART I									
(Column 1)		(Column 2)							
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)	
☐ BASIC FEE (37 CFR 1.16(a)(1)(i)-(iv))		N/A		N/A		N/A			
☐ SEARCH FEE (37 CFR 1.16(a)(1)(v)-(vi))		N/A		N/A		N/A			
☐ EXAMINATION FEE (37 CFR 1.16(a)(1)(vii)-(viii))		N/A		N/A		N/A			
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =		^		X \$		-	
INDEPENDENT CLAIMS (37 CFR 1.16(j))		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									
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	06/05/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	20	Minus	20	- 0	X \$40 -		0	
	Independent (37 CFR 1.16(j))	3	Minus	3	- 0	X \$210 -		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	
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))		Minus		-	X \$		-	
	Independent (37 CFR 1.16(j))		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.									

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.

DOCKET NO. 130839.00921

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Blair NICODEMUS et al.**

**Title: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO
COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES**

Application No.: **13/587,505**

Group Art Unit: **2431**

Filed: **August 16, 2012**

Examiner: **To Be Determined**

Confirmation: **9471**

Filed by EFS on: **June 6, 2013**

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

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

Sir:

Responsive to the Notice to File Corrected Application Papers dated April 10, 2013,
submitted herewith is the following:

- Replacement Sheets (7 Sheets)

The drawings are now compliant with 37 C.F.R. § 1.84.

No additional fees are believed to be due in connection with the filing of these papers.
The undersigned hereby authorizes the Commissioner to charge any shortage in fees due in
connection with the filing of this submission, including extension of time fees, to Deposit
Account No. 50-0436 and credit any excess fees to such deposit account.

Respectfully Submitted,

By: /Michael K. Jones, Reg. #41100/
Michael K. Jones
Registration No. 41,100

Dated: **June 6, 2013**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4405
Facsimile: (610) 640-7835

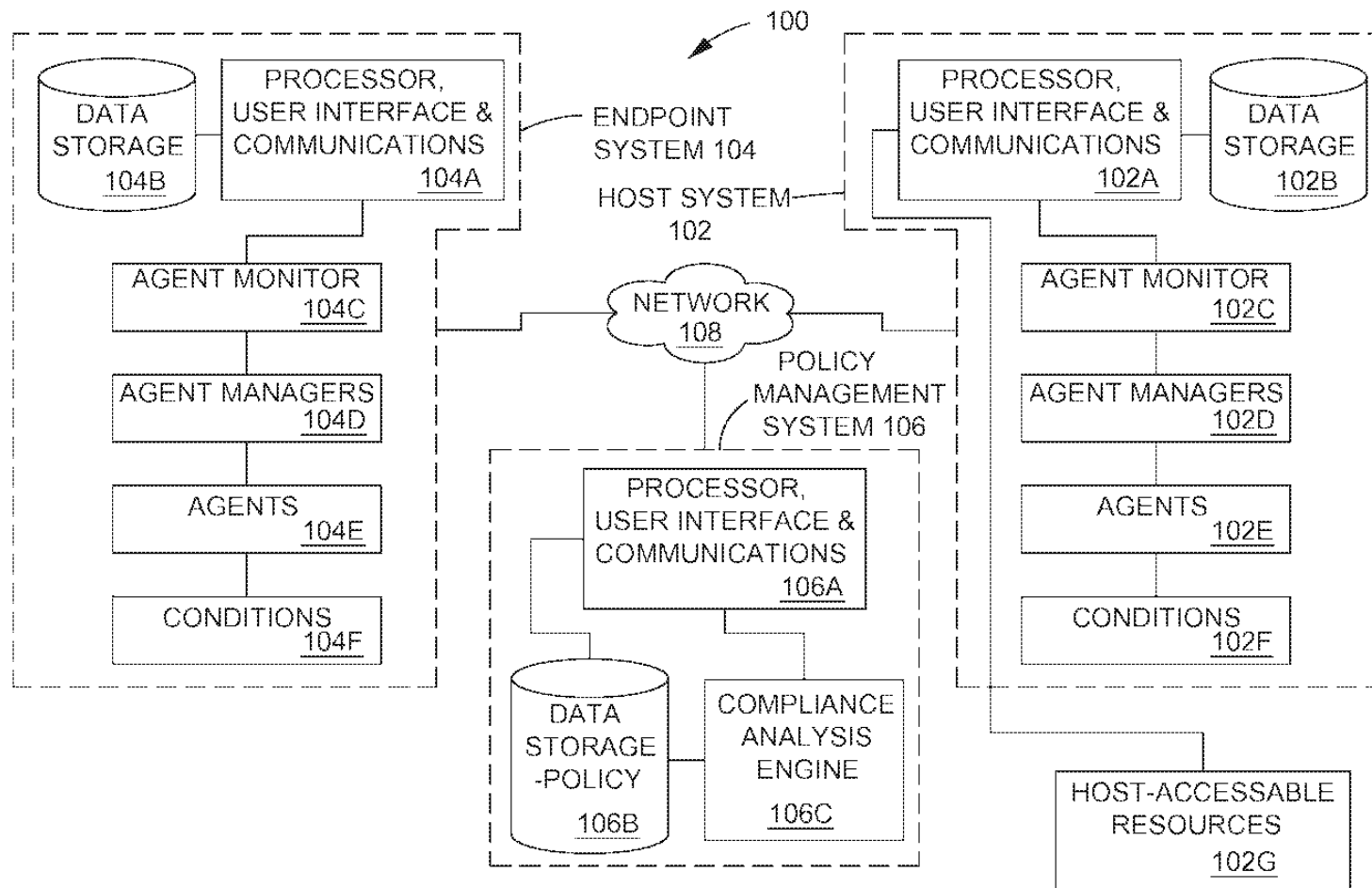


FIG. 1

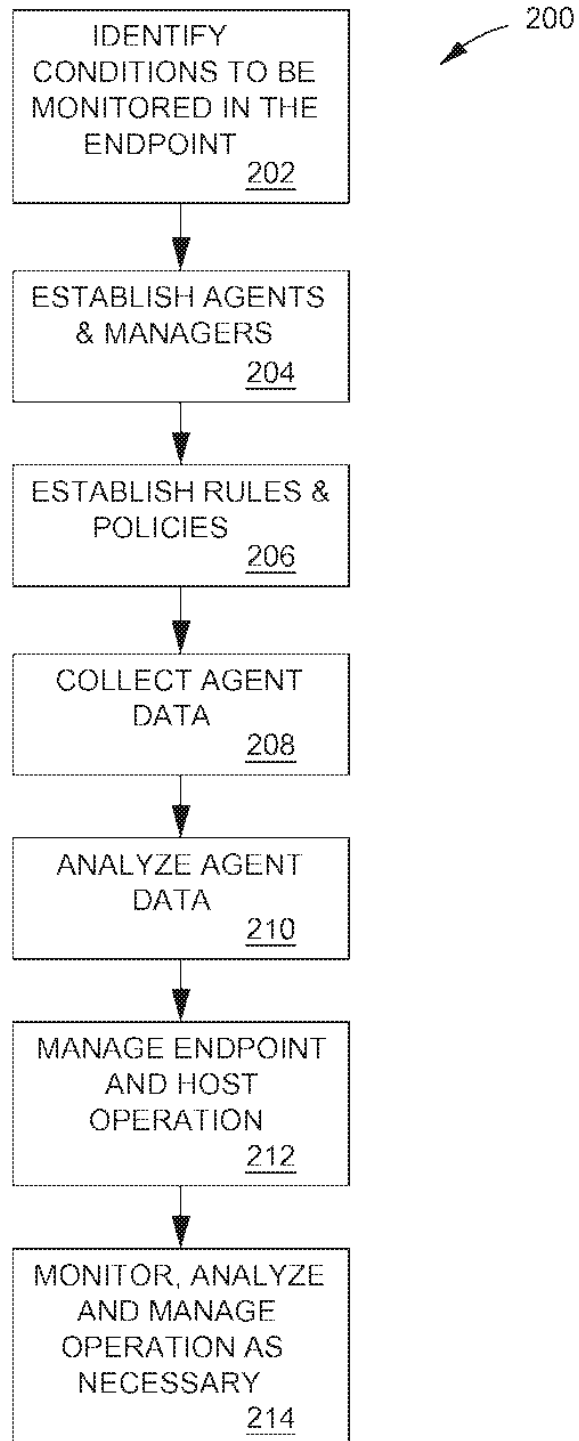


FIG. 2

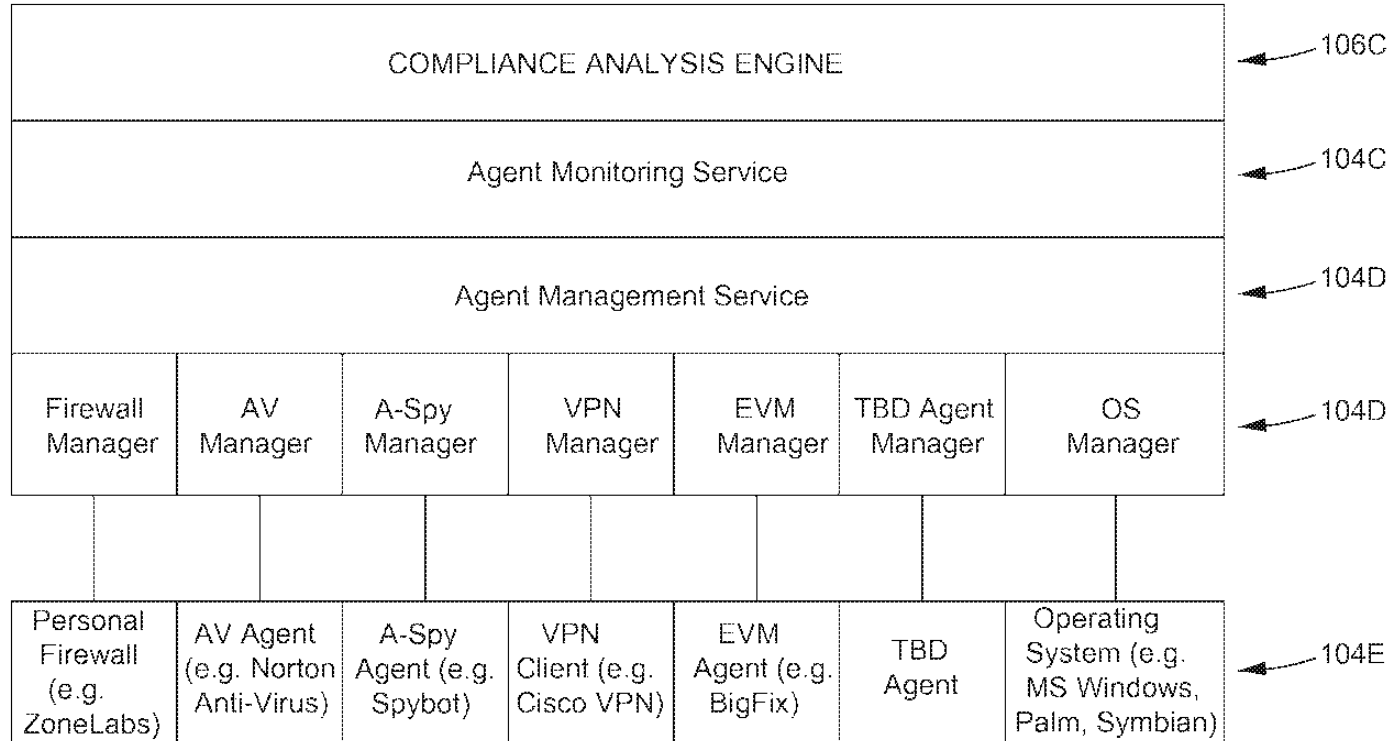


FIG. 3

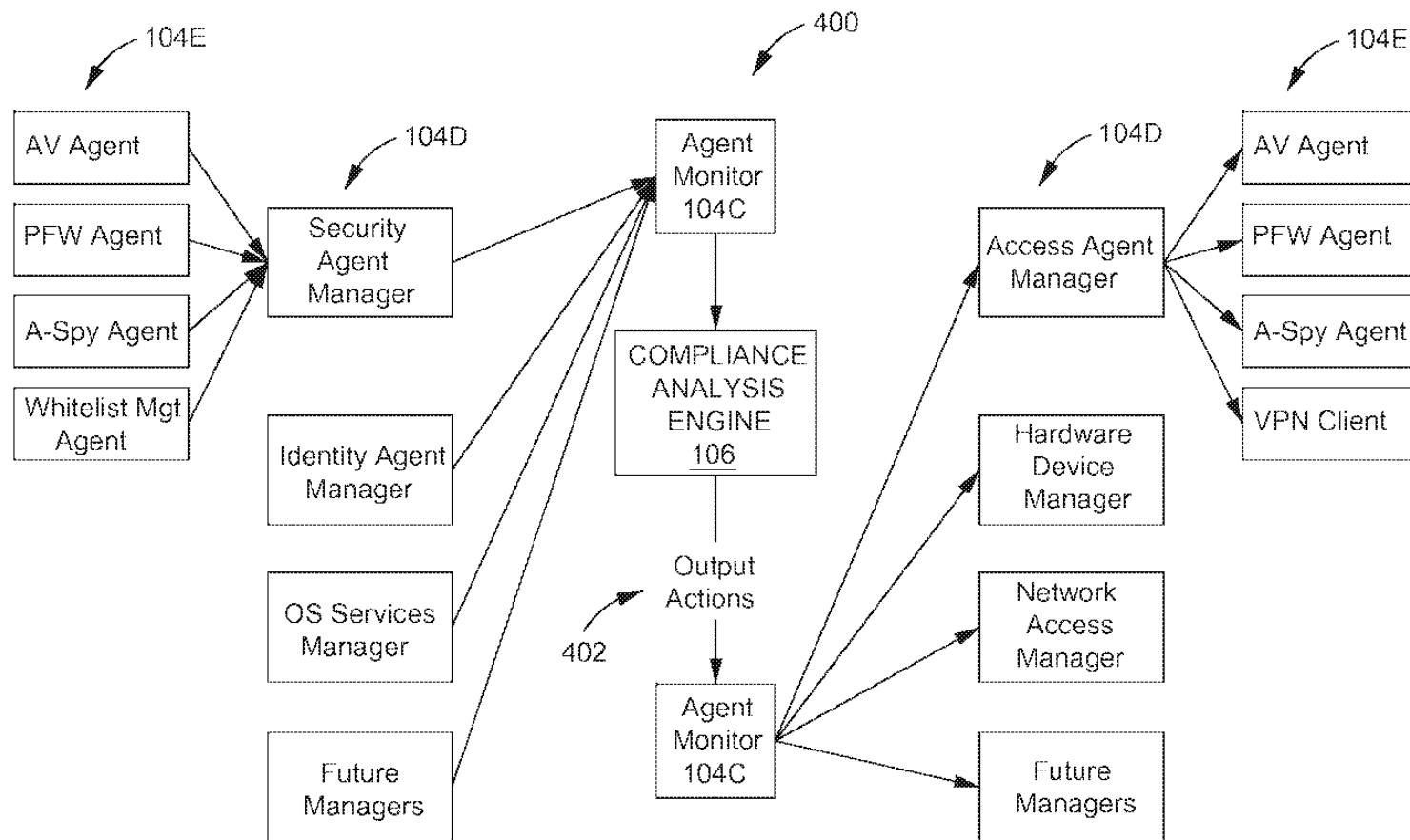


FIG. 4

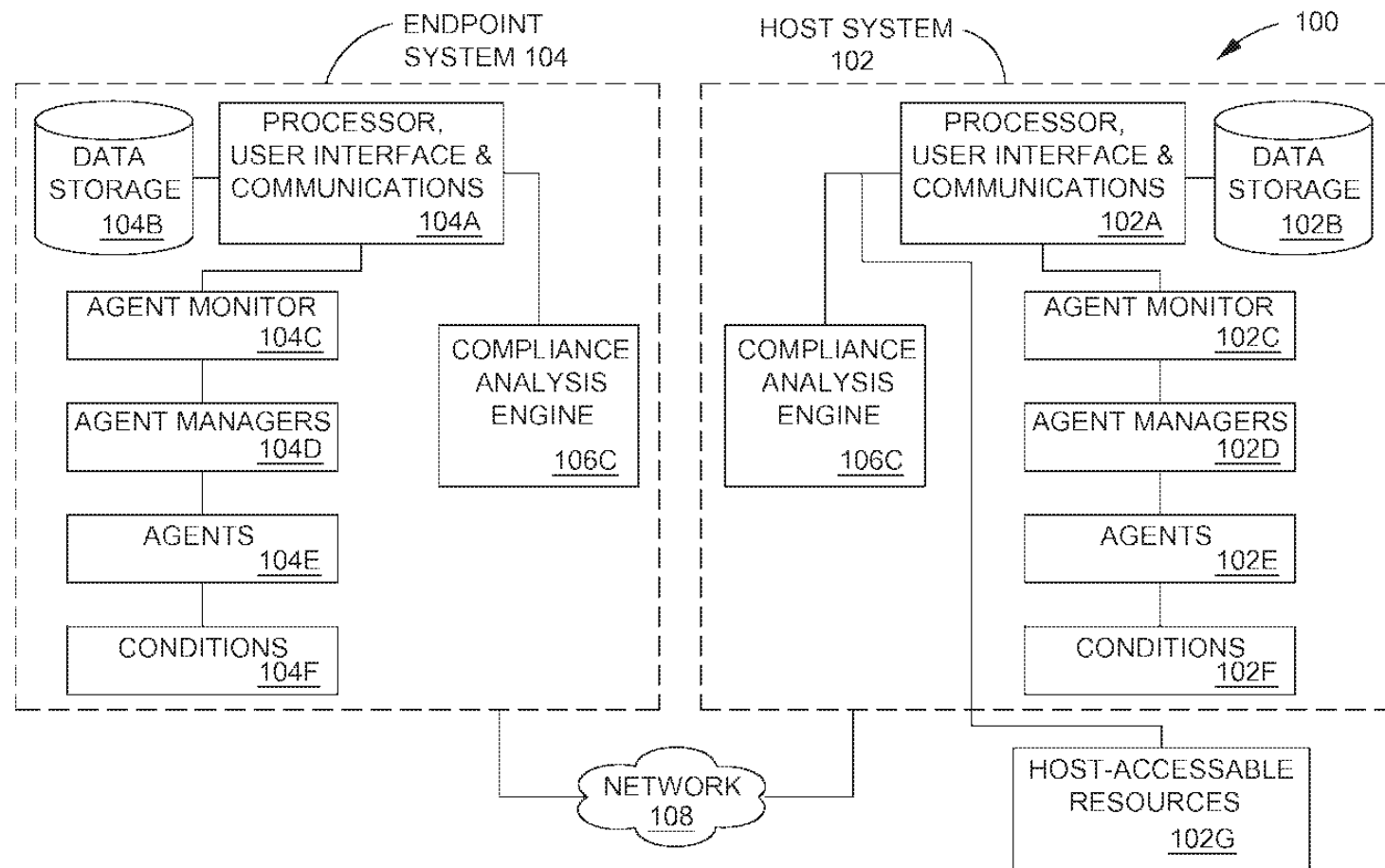


FIG. 5

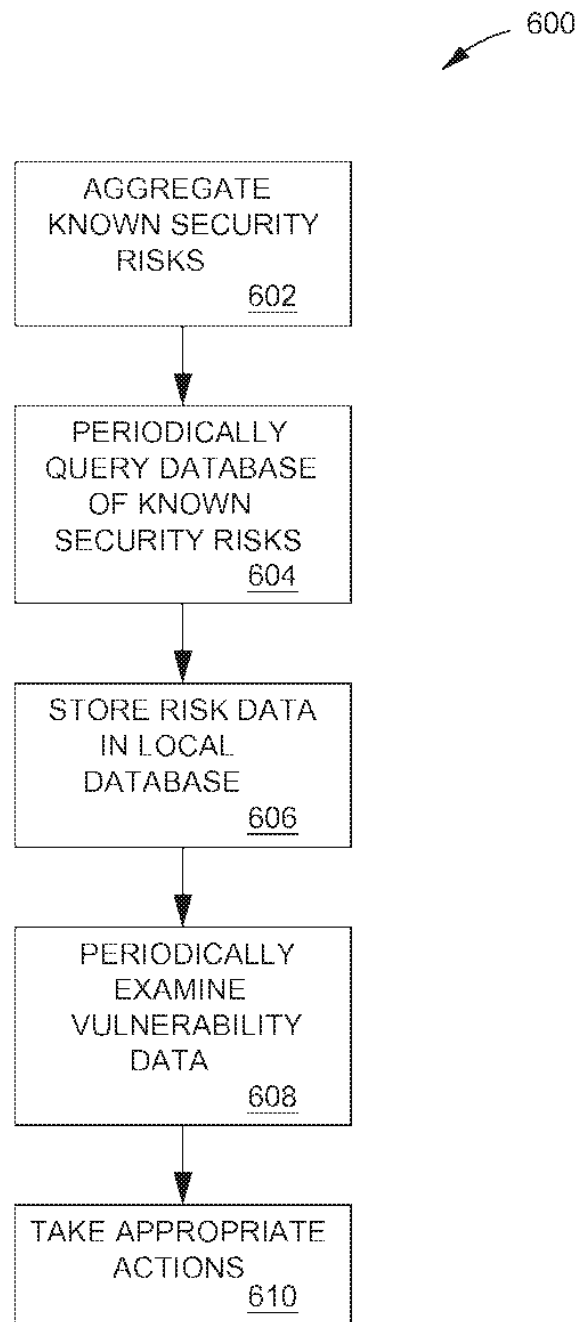


FIG. 6

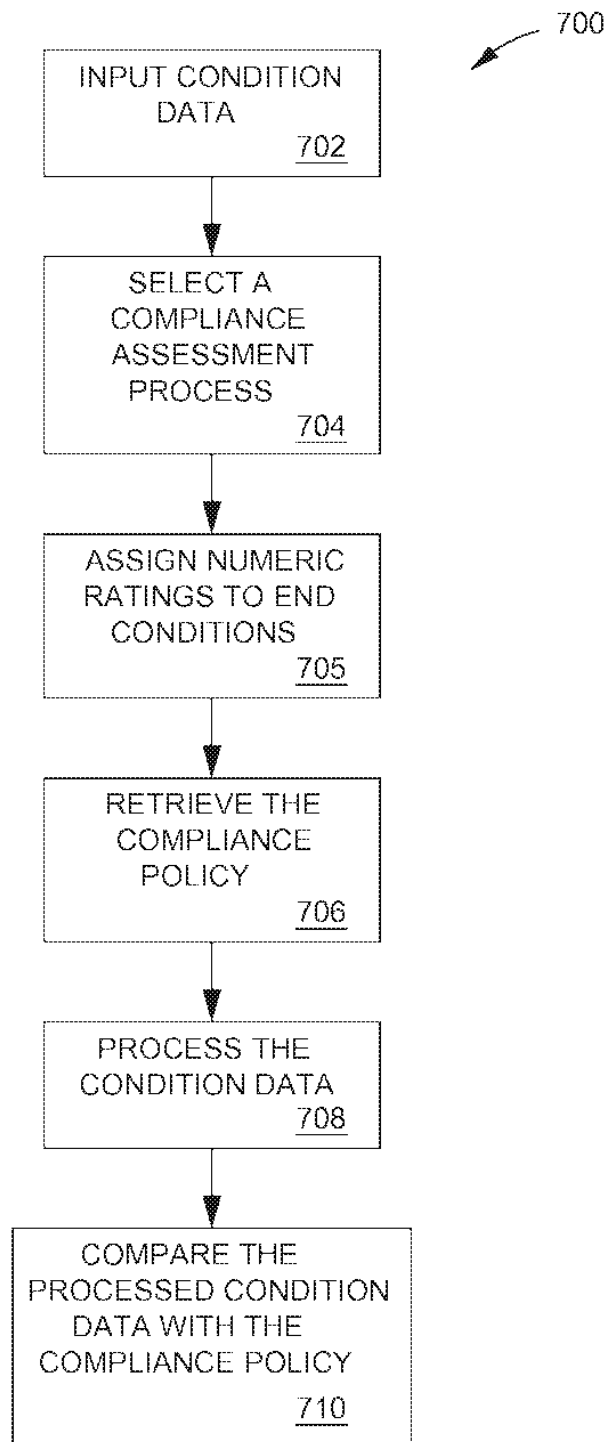


FIG. 7

Electronic Acknowledgement Receipt	
EFS ID:	15965200
Application Number:	13587505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair Nicodemus
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.00921
Receipt Date:	06-JUN-2013
Filing Date:	16-AUG-2012
Time Stamp:	13:06:49
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	Applicant Response to Pre-Exam Formalities Notice	921RES.pdf	85150 E3B067A8D47AEFCD8FB79238E7239D77	no	1

Warnings:

Information:

2	Drawings-only black and white line drawings	921DRAWINGS.pdf	55774 3c537ce4290ca7a3117436a889c4889ac79243a4e9ff	no	7
Warnings:					
Information:					
Total Files Size (in bytes):			140924		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.					
<u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.					
<u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.					
<u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Dossier Number 13/587,505								
APPLICATION AS FILED - PART I														
(Column 1) FOR		(Column 2) NUMBER FILED		(Column 2) NUMBER EXTRA		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY					
BASIC FEE <small>(37 CFR 1.16(a), (b), or (d))</small>		N/A		N/A		RATE(\$) N/A		FEE(\$) 70		RATE(\$) N/A		FEE(\$) N/A		
SEARCH FEE <small>(37 CFR 1.16(d), (e), or (f))</small>		N/A		N/A		N/A		300		N/A		N/A		
EXAMINATION FEE <small>(37 CFR 1.16(a), (b), or (d))</small>		N/A		N/A		N/A		360		N/A		N/A		
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>		33 minus 20 =		13		x 40		520		OR	N/A		N/A	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(i))</small>		3 minus 3 =		0		x 210 =		0.00		N/A		N/A		
APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>		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		0.00		N/A		N/A		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		0.00				0.00		0.00		N/A		N/A		
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL		1250		TOTAL		N/A		
APPLICATION AS AMENDED - PART II														
(Column 1) AMENDMENT A		(Column 2) CLAIMS REMAINING AFTER AMENDMENT		(Column 3) HIGHEST NUMBER PREVIOUSLY PAID FOR		(Column 3) PRESENT EXTRA		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY			
Total <small>(37 CFR 1.16(i))</small>		*		Minus **		RATE(S) x		ADDITIONAL FEE(S) N/A		OR	RATE(S) x		ADDITIONAL FEE(S) N/A	
Independent <small>(37 CFR 1.16(i))</small>		*		Minus ***		x =		N/A		OR	x =		N/A	
Application Size Fee (37 CFR 1.16(s))		N/A				N/A		N/A		OR	N/A		N/A	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))		N/A				N/A		N/A		OR	N/A		N/A	
TOTAL ADDL FEE						N/A		N/A		OR	TOTAL ADDL FEE		N/A	
(Column 1) AMENDMENT B		(Column 2) CLAIMS REMAINING AFTER AMENDMENT		(Column 3) HIGHEST NUMBER PREVIOUSLY PAID FOR		(Column 3) PRESENT EXTRA		SMALL ENTITY		OR	OTHER THAN SMALL ENTITY			
Total <small>(37 CFR 1.16(i))</small>		*		Minus **		x		N/A		OR	x =		N/A	
Independent <small>(37 CFR 1.16(i))</small>		*		Minus ***		x		N/A		OR	x =		N/A	
Application Size Fee (37 CFR 1.16(s))		N/A				N/A		N/A		OR	N/A		N/A	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))		N/A				N/A		N/A		OR	N/A		N/A	
TOTAL ADDL FEE						N/A		N/A		OR	TOTAL ADDL FEE		N/A	
* 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 figure 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: 1000 M Street, NE, Room 1000
Washington, DC 20536
Phone: (800) 786-9199
www.uspto.gov

APPLICATION NUMBER	FILING DATE	CLASS CODE	CLASS SUBCLASS	ATTY. DOK. NO.	TOTAL CLAIMS	IND. CLAIMS
13/587,505	08/16/2012	2431	1320	130839.00921	33	3

CONFIRMATION NO. 9471

UPDATED FILING RECEIPT



0000000061839503

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 06/17/2013

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)

Blair Nicodemus, North Wales, PA;
Billy Edison Stephens, West Chester, PA;

Applicant(s)

Blair Nicodemus, North Wales, PA;
Billy Edison Stephens, West Chester, PA;

Assignment For Published Patent Application

FIBERLINK COMMUNICATIONS CORPORATION, Blue Bell, PA

Power of Attorney: The patent practitioners associated with Customer Number 33893

Domestic Priority data as claimed by applicant

This application is a CON of 11/451,950 06/13/2006 ABN
which claims benefit of 60/752,424 12/21/2005

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: 08/27/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/587,505**

Projected Publication Date: 09/26/2013

Non-Publication Request: No

Early Publication Request: No

page 1 of 3

**** SMALL ENTITY ****

Title

METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES
BASED ON KNOWN SECURITY VULNERABILITIES

Preliminary Class

726

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

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).

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 Assets Control, 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.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: 400 M STREET, N.E., 3RD FLOOR
WASHINGTON, D.C. 20540
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR PRIORITY DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./FILE NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921

CONFIRMATION NO. 9471

PUBLICATION NOTICE



0000000064038428

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Title:METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES

Publication No.US-2013-0254833-A1

Publication Date:09/26/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505
	Filing Date		2012-08-16
	First Named Inventor	Blair Nicodemus	
	Art Unit	2438	
	Examiner Name	Josnel Jeudy	
	Attorney Docket Number	130839.00921	

U.S. PATENTS						
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	5666411		1997-09-09	McCarty	
	2	5673322		1997-09-30	Pepe et al.	
	3	5732074		1998-03-24	Spaur et al.	
	4	5987611		1999-11-16	Freund	
	5	6012100		2000-01-04	Frailong et al.	
	6	6061650		2000-05-09	Malkin et al.	
	7	6081508		2000-06-27	West et al.	
	8	6151628		2000-11-21	Xu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13587505
	Filing Date	2012-08-16
	First Named Inventor	Blair Nicodemus
	Art Unit	2438
	Examiner Name	Josnel Jeudy
	Attorney Docket Number	130839.00921

	9	6185609		2001-02-06	Rangarajan et al.	
	10	6253327		2001-06-26	Zhang et al.	
	11	6298445		2001-10-02	Shostack et al.	
	12	6377982		2002-04-23	Rai et al.	
	13	6453035		2002-09-17	Psarras et al.	
	14	6493349		2002-12-10	Casey	
	15	6539482		2003-03-25	Blanco et al.	
	16	6643782		2003-11-04	Jin et al.	
	17	6654891		2003-11-25	Borsato et al.	
	18	6694437		2004-02-17	Pao et al.	
	19	6732270		2004-05-04	Patzer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13587505
	Filing Date	2012-08-16
	First Named Inventor	Blair Nicodemus
	Art Unit	2438
	Examiner Name	Josnel Jeudy
	Attorney Docket Number	130839.00921

	20	6748543		2004-06-08	Vilhuber	
	21	6751729		2004-06-15	Ginger et al.	
	22	6760444		2004-07-06	Leung	
	23	6766453		2004-07-20	Nessett et al.	
	24	6778498		2004-08-17	McDysan	
	25	6785823		2004-08-31	Abrol et al.	
	26	6850943		2005-02-01	Teixeira et al.	
	27	6874139		2005-03-29	Krueger et al.	
	28	7058821		2006-06-06	Parekh et al.	
	29	7185192		2007-02-27	Kahn	
	30	7243148		2007-07-10	Keir et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

	31	7673323		2010-03-02	Moriconi	
	32	7805752		2010-09-28	Newstadt et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20020138756		2002-09-26	Makofka et al.	
	2	20020199203		2002-12-26	Duffey et al.	
	3	20030074580		2003-04-17	Knouse et al.	
	4	20030105978		2003-06-05	Byrne	
	5	20030135611		2003-07-17	Kemp et al.	
	6	20030172292		2003-09-11	Judge	
	7	20040005886		2004-01-08	Oda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13587505
	Filing Date	2012-08-16
	First Named Inventor	Blair Nicodemus
	Art Unit	2438
	Examiner Name	Josnel Jeudy
	Attorney Docket Number	130839.00921

	8	20040088565		2004-05-06	Norman et al.	
	9	20040107360		2004-06-03	Herrmann et al.	
	10	20040123162		2004-06-24	Antell et al.	
	11	20040167984		2004-08-26	Herrmann	
	12	20040193907		2004-09-30	Pantarella	
	13	20040221174		2004-11-04	Le Saint et al.	
	14	20050015622		2005-01-20	Williams et al.	
	15	20050033596		2005-02-10	Tummolo	
	16	20050044418		2005-02-24	Miliefsky	
	17	20050060537		2005-03-17	Stamos et al.	
	18	20050086511		2005-04-21	Balacheff et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505
	Filing Date		2012-08-16
	First Named Inventor	Blair Nicodemus	
	Art Unit	2438	
	Examiner Name	Josnel Jeudy	
	Attorney Docket Number	130839.00921	

	19	20050132225		2005-06-16	Gearhart	
	20	20050138408		2005-06-23	Vanover et al.	
	21	20050144475		2005-06-30	Sakaki et al.	
	22	20050154885		2005-07-14	Viscomi et al.	
	23	20050166065		2005-07-28	Eytchison et al.	
	24	20050172142		2005-08-04	Shelest et al.	
	25	20050188065		2005-08-25	O'Rourke et al.	
	26	20050223221		2005-10-06	Proudlar et al.	
	27	20050246767		2005-11-03	Fazal et al.	
	28	20070124803		2007-05-31	Taraz	
	29	20070143851		2007-06-21	Nicodemus et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505
	Filing Date		2012-08-16
	First Named Inventor	Blair Nicodemus	
	Art Unit	2438	
	Examiner Name	Josnel Jeudy	
	Attorney Docket Number	130839.00921	

	30	20070143827		2007-06-21	Nicodemus et al.	
--	----	-------------	--	------------	------------------	--

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2j}	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							☐

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

NON-PATENT LITERATURE DOCUMENTS

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 ⁶
	1	Introduction to Radius, Radius - GNU Project - Free Software Foundation (FSF), 5 pages.	☐
	2	Overview 1, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
	3	Overview 2, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
	4	Security Solutions that are Persistent and Pervasive...Yet Transparent to the End User, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
	5	Virtual Private Networking in Windows 2000: An Overview, Microsoft Windows 2000 Server (1999) 28 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13587505
	Filing Date	2012-08-16
	First Named Inventor	Blair Nicodemus
	Art Unit	2438
	Examiner Name	Josnel Jeudy
Attorney Docket Number		130839.00921

6	Wi-Fi Security at Work and on the Road, 5 pages.	☐
7	DAVIES, Joseph, Radius Protocol Security and Best Practices, Microsoft Windows 2000 Server (January 2002), 16 pages.	☐
8	TYSON, Jeff, How Virtual Private Networks Work, Howstuffworks, (07/12/2005), 10 pages.	☐
9	Novell eDirectory 8.7 Quick Look, http://www.novell.com/products/edirectory/quicklook.html , 2 pages.	☐
10	Novell eDirectory, Directory Services, Technical White Paper, www.novell.com , 23 pages.	☐
11	Novell Secure Login Features and Benefits, http://www.novell.com/products/securelogin/features.html , 2 pages.	☐
12	Novell Secure Login Quick Look, http://www.novell.com/products/securelogin/quicklook.html , 2 pages.	☐
13	International Search Report dated February 6, 2008 from PCT/US06/048720	☐

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

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 precode 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	13587505
	Filing Date	2012-08-16
	First Named Inventor	Blair Nicodemus
	Art Unit	2438
	Examiner Name	Josnel Jeudy
	Attorney Docket Number	130839.00921

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	/Michael K. Jones, Reg. #41100/	Date (YYYY-MM-DD)	2013-11-11
Name/Print	Michael K. Jones	Registration Number	41100

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 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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/48720

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 9/32 (2007.01)

USPC - 726/2

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 726/2

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/1, 2, 6 (text search)

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

Electronic databases: PubWEST(USPT,PGPB,EPAB,JPAB); DialogPRO; GoogleScholar

Search Terms Used: vulnerability, security, agent, update, status, state, policy etc.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 2005/0086511 A1 (BALACHEFF et al.) 21 April 2005 (21.04.2005), entire document (especially para [0003], [0011], [0014]-[0015], [0017], [0027], [0038]-[0044], [0063] and fig 1, 2)	1-5 and 10-23 ----- 6-9
X — Y	US 2005/0223221 A1 (PROUDLER et al.) 6 October 2005 (06.10.2005), entire document (para [0003], [0007], [0021]-[0022], [0026]-[0028], [0036], [0046], [0115], [0134]-[0147], [abstract], and fig 4, 5, 10, 11)	24-41 ----- 6-9
A	US 2005/0246767 A1 (FAZAL et al.) 3 November 2005 (03.11.2005), entire document	1-41

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

10 July 2007 (10.07.2007)

Date of mailing of the international search report

06 FEB 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

Electronic Acknowledgement Receipt	
EFS ID:	17366075
Application Number:	13587505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair Nicodemus
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.00921
Receipt Date:	11-NOV-2013
Filing Date:	16-AUG-2012
Time Stamp:	15:32:10
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	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	/9111 e3e77a: c0661e7: 9e6e525c302d8d16a: ce9889	no	10

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
2	Other Reference-Patent/App/Search documents	ISR.pdf	5208/ 0111a9d7c06c5da8d35a276b3a87cd0135 9712a	no	1
Warnings:					
Information:					
3	Non Patent Literature	NPL1.pdf	1953/8 9411a80f7c01e5827e201d07c1a5ed01f cc2	no	5
Warnings:					
Information:					
4	Non Patent Literature	NPL2.pdf	/6562 0951411caaf50ca7c6d5850c34e5d198 72d	no	2
Warnings:					
Information:					
5	Non Patent Literature	NPL3.pdf	61611 06485d3d7e0e9c5b5f0c7a01a0e1e25a2 50a3c	no	2
Warnings:					
Information:					
6	Non Patent Literature	NPL4.pdf	/3002 000d590c7d18a7a895653c2a02062f0e0 7d8d	no	2
Warnings:					
Information:					
7	Non Patent Literature	NPL5.pdf	1054562 477a0e141786721c550600ed0d1c757ce 009	no	28
Warnings:					
Information:					
8	Non Patent Literature	NPL6.pdf	226335 c271267a96ce7d6151a51515f0ed1a61 8428	no	5
Warnings:					
Information:					
9	Non Patent Literature	NPL7.pdf	54/448 50767a0d1058a76c22d065a1d2d06e0 75c1	no	16
Warnings:					
Information:					
10	Non Patent Literature	NPL8.pdf	495/9/ 3c15c5ad2f0c21d01f14e51e79dcd067e 41c9	no	10

Warnings:					
Information:					
11	Non Patent Literature	NPL9.pdf	69667 5c9c117a857a228ba2280c53b0baed768b56ac4	no	2
Warnings:					
Information:					
12	Non Patent Literature	NPL10.pdf	949343 3117a6e9bcb83b94c1187c0eccc0237773d405644	no	23
Warnings:					
Information:					
13	Non Patent Literature	NPL11.pdf	70281 a13ca19c0edf246a5dfe1a5778d17884e9c04	no	2
Warnings:					
Information:					
14	Non Patent Literature	NPL12.pdf	62808 12e8b1dc77a811c11c9b0c5a5b02174c46c4d	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			4013992		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 2489
Alexandria, Virginia 22304-2489
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921	9471
85398 7899 03/04/2014 Pepper Hamilton LLP 400 Berywn Park 899 Cassatt Road Berwyn, PA 19312-1183			EXAMINER JUDY COSNELL	
			ART UNIT 2-38	PAPER NUMBER
			MAIL DATE 03/04/2014	DELIVERY MODE 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.

Office Action Summary

Application No.
13/587,505

Examiner
JOSNEL JEUDY

Applicant(s)
NICODEMUS ET AL.

Art Unit
2438

AIA (First Inventor to File)
Status
No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.135(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- THE period for reply is specified above; the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office after three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.104(b).

Status

- ☒ Responsive to communication(s) filed on 08/16/2012.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- ☒ Claim(s) 1-63 is/are pending in the application.
5a) Of the above claim(s) 1-30 is/are withdrawn from consideration.
- 6) ☐ Claim(s) _____ is/are allowed.
- 7) ☒ Claim(s) 31-63 is/are rejected.
- 8) ☐ Claim(s) _____ is/are objected to.
- 9) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 06/06/2013 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- ☐ All
- ☐ Some**
- ☐ None of the:
 - ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 11/11/2013
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 4) ☐ Other: _____

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

This action is responsive to the communication filed on August 16, 2012. At this time, claims 1-30 have been cancelled. Claims 31- 63 are pending and addressed below.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 53-63 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Each element of the claim can reasonably be interpreted as software. Absent a controlling definition in the specification, a reasonable interpretation of a processor is just a software routine. The preamble recites a system but a system is just a collection of elements and software is an element. This claim fails to fall into a statutory category of invention as software alone is not a machine, a manufacture, a process nor a composition matter.

Claim Rejections - 35 USC § 102

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

A person shall be entitled to a patent unless –

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

Claims 31-33, 36-39, 41-44, 47-50, 52-55, 58-61 and 63 are rejected under 35 U.S.C 102(e) as being anticipated over Balacheff US pat. No 20050086511 (IDS Submitted, 11/11/2013).

Regarding claim 31, Balacheff discloses a method for controlling the operation of an endpoint, **(See Balacheff, abstract; seeks information about the ability of the second data processing device to respect conditions specified in the policy)** comprising:

providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; **(See Balacheff, fig 1, computer 6 has an interface and [0003]; the first data processing device has a first policy associated with it)**

maintaining the plurality of policies in a data store on the computing system; **(See Balacheff, fig 1 and [0039]; policies are stored within element 12 of computer 6)**

identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor; **(See Balacheff, [0042]; the trusted component 30, which is typically a tamper resistant hardware component which is manufactured in accordance with strict rules and whose operation is assured because its internal computational processes cannot be subverted, monitors the files and/or data contained within the BIOS and operating system of the computer. The monitoring is dynamic and allows measurements of the computing environment to be made. Thus, for example, before the BIOS routines are executed the trusted component 30 may examine the BIOS and calculate a integrity metric, for example a hash of the BIOS, which can be stored within a memory controlled by the trusted component 30 along with an indication of the current BIOS version within the computer 20. Similarly, as the operating system starts to build integrity measurements of the operating**

system may be made and stored in a log together with an indication of the components within the operating system. Thus the trusted computing device has a running log of the state of the system and the integrity metrics for the system at any given time.)

configuring one or more agents on the endpoint to monitor the plurality of conditions; **(See Balacheff, [0042]; the trusted component 30, monitors the files and/or data contained within the BIOS and operating system of the computer. The monitoring is dynamic and allows measurements of the**

computing environment to be made. Thus, for example, before the BIOS routines are executed the trusted component 30 may examine the BIOS and calculate a integrity metric, for example a hash of the BIOS, which can be stored within a memory controlled by the trusted component 30 along with an indication of the current BIOS version within the computer 20. Similarly, as the operating system starts to build integrity measurements of the operating system may be made and stored in a log together with an indication of the components within the operating system. Thus the trusted computing device has a running log of the state of the system and the integrity metrics for the system at any given time)

receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more agents; (See Balacheff, [0044]; Once communication has been established, the processor 14 instructs the data processor 8 to communicate with the trusted component 30 so as to obtain the log of the components installed within the computer 20 together with the integrity metrics)

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; (See Balacheff, [0044]; once communications between the computers 20 and 6 have been established decisions concerning further access of data by the computer 20 within the memory 4 of the computer 6 are made by the policy processor 14. Its user will probably release its integrity metric for evaluation. The first computer starts the step of obtaining information about the second computing device and in particular its ability to respect and uphold any policies that are associated with the data items. Once the state of the second computer 20 has been made available to the policy processor 14 it can then check to see what level of access it should grant either to the directory structure within the memory 4 or to individual files)

and initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store. (See Balacheff, [0044]; an attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these

circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)

Regarding claim 32, Balacheff discloses the method of claim 31, wherein the action comprises controlling access of the endpoint to computing resources. **(See Balacheff, [0044]; an attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)**

Regarding claim 33, Balacheff discloses the method of claim 31, wherein the user interface comprises a web page. **(See Balacheff, [0064]; web –based service)**

Regarding claim 36, Balacheff discloses the method of claim 31, wherein the plurality of agents comprise at least one service provided by the operating system of the endpoint. **(See Balacheff, [0042]; the operating system starts to build integrity measurements of the operating system may be made)**

Regarding claim 37, Balacheff discloses the method of claim 31, wherein the plurality of agents comprise at least one application running on the endpoint. **(See Balacheff, [0042]; an application)**

Regarding claim 38, Balacheff discloses the method of claim 31, wherein the conditions comprise at least one hardware condition. **(See Balacheff, [0044]; information about the computing device)**

Regarding claim 39, Balacheff discloses the method of claim 31, wherein the conditions comprise at

least one software condition. **(See Balacheff, [0042]; the log can contain the identity and version number of each procedure, application, DLL and so on)**

Regarding claim 41, Balacheff discloses the method of claim 31, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action. **(See Balacheff, [0044]; the policy processor may operate at many levels. Thus it may be sufficient that the second computer is operating on a specified operating system as that may in itself be deemed to have sufficient intrinsic policy enforcement processes to allow the data to be made available to the second computer. An attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)**

Regarding claim 42, Balacheff discloses a non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, **(See Balacheff, abstract; seeks information about the ability of the second data processing device to respect conditions specified in the policy)** comprising:

providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; **(See Balacheff, fig 1, computer 6 has an interface and [0003]; the first data processing device has a first policy associated with it)**

maintaining the plurality of policies in a data store on the computing system; **(See Balacheff, fig 1 and [0039]; policies are stored within element 12 of computer 6)**

identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor; **(See Balacheff, [0042]; the trusted component 30, which is typically a tamper resistant hardware component which is manufactured in accordance with strict rules and whose operation is assured**

because its internal computational processes cannot be subverted, monitors the files and/or data contained within the BIOS and operating system of the computer. The monitoring is dynamic and allows measurements of the computing environment to be made. Thus, for example, before the BIOS routines are executed the trusted component 30 may examine the BIOS and calculate a integrity metric, for example a hash of the BIOS, which can be stored within a memory controlled by the trusted component 30 along with an indication of the current BIOS version within the computer 20. Similarly, as the operating system starts to build integrity measurements of the operating system may be made and stored in a log together with an indication of the components within the operating system. Thus the trusted computing device has a running log of the state of the system and the integrity metrics for the system at any given time.)

configuring one or more agents on the endpoint to monitor the plurality of conditions; (See Balacheff, [0042]; the trusted component 30, monitors the files and/or data contained within the BIOS and operating system of the computer. The monitoring is dynamic and allows measurements of the computing environment to be made. Thus, for example, before the BIOS routines are executed the trusted component 30 may examine the BIOS and calculate a integrity metric, for example a hash of the BIOS, which can be stored within a memory controlled by the trusted component 30 along with an indication of the current BIOS version within the computer 20. Similarly, as the operating system starts to build integrity measurements of the operating system may be made and stored in a log together with an indication of the components within the operating system. Thus the trusted computing device has a running log of the state of the system and the integrity metrics for the system at any given time)

receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more agents; (See Balacheff, [0044]; Once communication has been established, the processor 14 instructs the data processor 8 to communicate with the trusted component 30 so as to obtain the log of the components installed within the computer 20 together with the integrity metrics)

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; **(See Balacheff, [0044]; once communications between the computers 20 and 6 have been established decisions concerning further access of data by the computer 20 within the memory 4 of the computer 6 are made by the policy processor 14. Its user will probably release its integrity metric for evaluation. The first computer starts the step of obtaining information about the second computing device and in particular its ability to respect and uphold any policies that are associated with the data items. Once the state of the second computer 20 has been made available to the policy processor 14 it can then check to see what level of access it should grant either to the directory structure within the memory 4 or to individual files)**

and initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store. **(See Balacheff, [0044]; an attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)**

Regarding claim 43, Balacheff discloses the computer readable medium of claim 42, wherein the action comprises controlling access of the endpoint to computing resources. (See Balacheff, [0044]; an attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that

the second computer is, or can be placed in, a sufficiently trusted state)

Regarding claim 44, Balacheff discloses the computer readable medium of claim 42, wherein the user interface comprises a web page. **(See Balacheff, [0064]; web –based service)**

Regarding claim 47, Balacheff discloses the computer readable medium of claim 42, wherein the plurality of agents comprise at least one service provided by the operating system of the endpoint. **(See Balacheff, [0042]; the operating system starts to build integrity measurements of the operating system may be made)**

Regarding claim 48, Balacheff discloses the computer readable medium of claim 42, wherein the plurality of agents comprise at least one application running on the endpoint. **(See Balacheff, [0042]; an application)**

Regarding claim 49, Balacheff discloses the computer readable medium of claim 42, wherein the conditions comprise at least one hardware condition. **(See Balacheff, [0044]; information about the computing device)**

Regarding claim 50, Balacheff discloses the computer readable medium of claim 42, wherein the conditions comprise at least one software condition. **(See Balacheff, [0042]; the log can contain the identity and version number of each procedure, application, DLL and so on)**

Regarding claim 52, Balacheff discloses the computer readable medium of claim 42, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action. **(See Balacheff, [0044]; the policy processor may operate at many levels. Thus it may be sufficient that the second computer is operating on a specified operating system as that may in itself be deemed to have sufficient intrinsic policy enforcement processes to allow the data to be made**

available to the second computer. An attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)

Regarding claim 53, Balacheff discloses a system for controlling the operation of an endpoint, (See Balacheff, abstract; seeks information about the ability of the second data processing device to respect conditions specified in the policy) comprising:

a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; (See Balacheff, fig 1, computer 6 has an interface and [0003]; the first data processing device has a first policy associated with it)

a data store, at the computing system, that contains the plurality of policies; (See Balacheff, fig 1 and [0039]; policies are stored within element 12 of computer 6)

one or more agents on the endpoint configured to monitor a plurality of conditions identified in the plurality of policies; (See Balacheff, [0042]; the trusted component 30,monitors the files and/or data contained within the BIOS and operating system of the computer. The monitoring is dynamic and allows measurements of the computing environment to be made. Thus, for example, before the BIOS routines are executed the trusted component 30 may examine the BIOS and calculate a integrity metric, for example a hash of the BIOS, which can be stored within a memory controlled by the trusted component 30 along with an indication of the current BIOS version within the computer 20. Similarly, as the operating system starts to build integrity measurements of the operating system may be made and stored in a log together with an indication of the components within the operating system. Thus the trusted computing device has a running log of the state of the system and the integrity metrics for the system at any given time)

and one or more processors at the computing system (See Balacheff, fig 1 and fig 2) configured to:

receive, across a network, status information about the plurality of conditions on the endpoint gathered by the one or more agents, **(See Balacheff, [0044]; Once communication has been established, the processor 14 instructs the data processor 8 to communicate with the trusted component 30 so as to obtain the log of the components installed within the computer 20 together with the integrity metrics)**

determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, **(See Balacheff, [0044]; once communications between the computers 20 and 6 have been established decisions concerning further access of data by the computer 20 within the memory 4 of the computer 6 are made by the policy processor 14. Its user will probably release its integrity metric for evaluation. The first computer starts the step of obtaining information about the second computing device and in particular its ability to respect and uphold any policies that are associated with the data items. Once the state of the second computer 20 has been made available to the policy processor 14 it can then check to see what level of access it should grant either to the directory structure within the memory 4 or to individual files)** and initiate, based on the compliance state, an action identified in at least one rule in the data store. **(See Balacheff, [0044]; an attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)**

Regarding claim 54, Balacheff discloses the system of claim 53, wherein the action comprises controlling access of the endpoint to computing resources. **(See Balacheff, [0044]; an attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be allowed to access the more sensitive data item. Under these circumstances the first computer can request additional**

information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)

Regarding claim 55, Balacheff discloses the system of claim 53, wherein the user interface comprises a web page. (See Balacheff, [0064]; web –based service)

Regarding claim 58, Balacheff discloses the system of claim 53, wherein the plurality of agents comprise at least one service provided by the operating system of the endpoint. (See Balacheff, [0042]; the operating system starts to build integrity measurements of the operating system may be made)

Regarding claim 59, Balacheff discloses the system of claim 53, wherein the plurality of agents comprise at least one application running on the endpoint. (See Balacheff, [0042]; an application)

Regarding claim 60, Balacheff discloses the system of claim 53, wherein the conditions comprise at least one hardware condition. (See Balacheff, [0044]; information about the computing device)

Regarding claim 61, Balacheff discloses the system of claim 53, wherein the conditions comprise at least one software condition. (See Balacheff, [0042]; the log can contain the identity and version number of each procedure, application, DLL and so on)

Regarding claim 63, Balacheff discloses the system of claim 53, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action. (See Balacheff, [0044]; the policy processor may operate at many levels. Thus it may be sufficient that the second computer is operating on a specified operating system as that may in itself be deemed to have sufficient intrinsic policy enforcement processes to allow the data to be made available to the second computer. An attempt to access a more sensitive data item may result in the first computer 6 determining that it has insufficient information to determine if the second computer can be

allowed to access the more sensitive data item. Under these circumstances the first computer can request additional information, or even down load security programs to the second computer in an attempt to ensure that the second computer is, or can be placed in, a sufficiently trusted state)

Claims 34-35, 45-46, and 56-57 are rejected under 35 U.S.C 103(a) as being unpatentable over Balacheff US pat. No 20050086511 (IDS Submitted, 11/11/2013), in view of Newstadt US pat. No 7805752. (IDS Submitted, 11/11/2013).

Regarding claim 34, Balacheff does not appear to explicitly disclose the method of claim 31, further comprising requesting, at the computing system, the status information on a periodic basis. However, Newstadt discloses further comprising requesting, at the computing system, the status information on a periodic basis. **(See Newstadt, Col 2, lines 35-52; a request for updated policies can be made periodically)**

Balacheff and Newstadt are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Newstadt to include the periodic update because it would have allowed the system to determine the state of the system in a periodic basis.

Regarding claim 35, Balacheff does not appear to explicitly disclose the method of claim 31, wherein the endpoint comprises a mobile device.

However, Newstadt discloses wherein the endpoint comprises a mobile device. **(See Newstadt, Col 7, lines 10-15; Smart phone)**

Balacheff and Newstadt are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Newstadt to include the smart phone because it would have allowed the user to use the device anywhere.

Regarding claim 45, Balacheff does not appear to explicitly disclose the computer readable medium of claim 42, further comprising requesting, at the computing system, the status information on a periodic basis.

However, Newstadt discloses further comprising requesting, at the computing system, the status information on a periodic basis. **(See Newstadt, Col 2, lines 35-52; a request for updated policies can be made periodically)**

Balacheff and Newstadt are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Newstadt to include the periodic update because it would have allowed the system to determine the state of the system in a periodic basis.

Regarding claim 46, Balacheff does not appear to explicitly disclose the computer readable medium of claim 42, wherein the endpoint comprises a mobile device.

However, Newstadt discloses wherein the endpoint comprises a mobile device. **(See Newstadt, Col 7, lines 10-15; Smart phone)**

Balacheff and Newstadt are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Newstadt to include the smart phone because it would have allowed the user to use the device anywhere.

Regarding claim 56, Balacheff does not appear to explicitly disclose the system of claim 53, wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis.

However, Newstadt discloses wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis. **(See Newstadt, Col 2, lines 35-52; a request for updated policies can be made periodically)**

Balacheff and Newstadt are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Newstadt to include the periodic update because it would have allowed the system to determine the state of the system in a periodic basis.

Regarding claim 57, Balacheff does not appear to explicitly disclose the system of claim 53, wherein the endpoint comprises a mobile device.

However, Newstadt discloses wherein the endpoint comprises a mobile device. **(See Newstadt, Col 2, lines 35-52; a request for updated policies can be made periodically)**

Balacheff and Newstadt are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Newstadt to include the periodic update because it would have allowed the system to determine the state of the system in a periodic basis.

Claims 40, 51 and 62 are rejected under 35 U.S.C 103(a) as being unpatentable over Balacheff US pat. No 20050086511 (IDS Submitted, 11/11/2013) in view of Taraz US pat. No 20070124803. (IDS Submitted, 11/11/2013).

Regarding claim 40, Balacheff does not appear to explicitly disclose the method of claim 31, wherein the computing system comprises a plurality of servers.

However, Taraz discloses wherein the computing system comprises a plurality of servers. **(See Taraz, [0020]; the AAA server 24 may operate in tandem with a Light-Weight Directory Access Protocol (LDAP)/Remote Dial-In User Access Server (RADIUS) server 26 configured to facilitate remote access to the network)**

Balacheff and Taraz are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention

was made to modify the invention of Balacheff with the teaching of Taraz to include the plurality of servers because it would have allowed a reliable system of the compliance system.

Regarding claim 51, Balacheff does not appear to explicitly disclose the computer readable medium of claim 42, wherein the computing system comprises a plurality of servers.

However, Taraz discloses wherein the computing system comprises a plurality of servers. **(See Taraz, [0020]; the AAA server 24 may operate in tandem with a Light-Weight Directory Access Protocol (LDAP)/Remote Dial-In User Access Server (RADIUS) server 26 configured to facilitate remote access to the network)**

Balacheff and Taraz are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Taraz to include the plurality of servers because it would have allowed a reliable system of the compliance system.

Regarding claim 62, Balacheff does not appear to explicitly disclose the system of claim 53, wherein the computing system comprises a plurality of servers.

However, Taraz discloses wherein the computing system comprises a plurality of servers. **(See Taraz, [0020]; the AAA server 24 may operate in tandem with a Light-Weight Directory Access Protocol (LDAP)/Remote Dial-In User Access Server (RADIUS) server 26 configured to facilitate remote access to the network)**

Balacheff and Taraz are analogous art because they are from the same field of endeavor which is compliance. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the invention of Balacheff with the teaching of Taraz to include the plurality of servers because it would have allowed a reliable system of the compliance system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOSNEL JEUDY whose telephone number is (571)270-7476. The examiner can normally be reached on 5/4/9.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Date: 02/18/2014

/JOSNEL JEUDY/
Examiner, Art Unit 2438

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	7	"20030014623"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/14 13:14
S2	6	"20050086511"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/14 13:33
S3	3	"20050223221"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/14 14:04
S4	3	"20050246767"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/14 15:21
S5	37619	(client or terminal or host or endpoint or workstation or device or computer) near5 (monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/14 16:21
S6	1158	(client or terminal or host or endpoint or workstation or device or computer) near5 (monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/14 16:22
S7	163	(client or terminal or host or endpoint or workstation or device or computer) near5 (monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) and (compliant or compliance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/14 16:22
S8	27367	(726/22-30).CCLS.	US-PGPUB;	OR	OFF	2014/02/14

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			16:24
S9	163	S6 and S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/14 16:24
S10	11	S7 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/14 16:25
S11	371	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/15 22:18
S12	27430	(726/22-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/02/15 22:20
S13	6	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance) and S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/15 22:20
S14	15	"7805752"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/18 15:21
S15	5	"20070124803"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 13:30
S16	3	"13587505"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	NEAR	OFF	2014/02/19 14:04

			IBM_TDB			
S17	1721	h04l67/1012.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:37
S18	45115	h04l67/10S.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:38
S19	87	h04l29/08189.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:38
S20	14783	h04l29/08S.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:38
S21	18	h04l29/06823\$.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:40
S22	13998	h04l63/10.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:40
S23	10058	h04l63/20.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/02/19 14:40
S24	0	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance) and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:46
S25	3	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or	US-PGPUB; USPAT; USOCR; FPRS; EPO;	NEAR	ON	2014/02/19 14:46

		device or computer) with (access\$3) and (compliant or compliance) and S18	JPO; DERWENT; IBM_TDB			
S26	0	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance) and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:46
S27	0	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance) and S20	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:46
S28	0	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance) and S21	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:46
S29	97	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance) and S22	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:46
S30	27	(monitor) near7 (condition or state or policy or polic\$3 or compliant or compliance) with (client or terminal or host or endpoint or workstation or device or computer) with (access\$3) and (compliant or compliance)and S23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:47
S31	988	(client or terminal or host or endpoint or workstation or device or computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S23	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:53
S32	1005	(client or terminal or host or endpoint or workstation or device or computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S22	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:54
S33	0	(client or terminal or host or endpoint or workstation or device or computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S21	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:54
S34	199	(client or terminal or host or endpoint or workstation or device or	US-PGPUB; USPAT;	NEAR	ON	2014/02/19 14:54

		computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S20	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S35	1	(client or terminal or host or endpoint or workstation or device or computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:54
S36	1606	(client or terminal or host or endpoint or workstation or device or computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:55
S37	143	(client or terminal or host or endpoint or workstation or device or computer)with (condition or state or policy or polic\$3 or compliant or compliance) with (access\$3) with (resource or content or data or information)and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	ON	2014/02/19 14:55

2/23/2014 9:16:50 PM

C:\Users\jjendy\Documents\EAST\Workspaces\13587505c.wsp

Receipt date: 11/11/2013

13587505 - GAU: 2438

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

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		13587505
	Filing Date		2012-08-16
	First Named Inventor	Blair Nicodemus	
	Art Unit	2438	
	Examiner Name	Josnel Jeudy	
	Attorney Docket Number	130839.00921	

U.S.PATENTS						
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
/J.J./	1	5666411		1997-09-09	McCarty	
/J.J./	2	5673322		1997-09-30	Pepe et al.	
/J.J./	3	5732074		1998-03-24	Spaur et al.	
/J.J./	4	5987611		1999-11-16	Freund	
/J.J./	5	6012100		2000-01-04	Frailong et al.	
/J.J./	6	6061650		2000-05-09	Malkin et al.	
/J.J./	7	6081508		2000-06-27	West et al.	
/J.J./	8	6151628		2000-11-21	Xu et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	9	6185609		2001-02-06	Rangarajan et al.	
/J.J./	10	6253327		2001-06-26	Zhang et al.	
/J.J./	11	6298445		2001-10-02	Shostack et al.	
/J.J./	12	6377982		2002-04-23	Rai et al.	
/J.J./	13	6453035		2002-09-17	Psarras et al.	
/J.J./	14	6493349		2002-12-10	Casey	
/J.J./	15	6539482		2003-03-25	Blanco et al.	
/J.J./	16	6643782		2003-11-04	Jin et al.	
/J.J./	17	6654891		2003-11-25	Borsato et al.	
/J.J./	18	6694437		2004-02-17	Pao et al.	
/J.J./	19	6732270		2004-05-04	Patzer et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	20	6748543		2004-06-08	Vilhuber	
/J.J./	21	6751729		2004-06-15	Ginger et al.	
/J.J./	22	6760444		2004-07-06	Leung	
/J.J./	23	6766453		2004-07-20	Nessett et al.	
/J.J./	24	6778498		2004-08-17	McDysan	
/J.J./	25	6785823		2004-08-31	Abrol et al.	
/J.J./	26	6850943		2005-02-01	Teixeira et al.	
/J.J./	27	6874139		2005-03-29	Krueger et al.	
/J.J./	28	7058821		2006-06-06	Parekh et al.	
/J.J./	29	7185192		2007-02-27	Kahn	
/J.J./	30	7243148		2007-07-10	Keir et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	31	7673323		2010-03-02	Moriconi	
/J.J./	32	7805752		2010-09-28	Newstadt et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/J.J./	1	20020138756		2002-09-26	Makofka et al.	
/J.J./	2	20020199203		2002-12-26	Duffey et al.	
/J.J./	3	20030074580		2003-04-17	Knouse et al.	
/J.J./	4	20030105978		2003-06-05	Byrne	
/J.J./	5	20030135611		2003-07-17	Kemp et al.	
/J.J./	6	20030172292		2003-09-11	Judge	
/J.J./	7	20040005886		2004-01-08	Oda et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	8	20040088565		2004-05-06	Norman et al.	
/J.J./	9	20040107360		2004-06-03	Herrmann et al.	
/J.J./	10	20040123162		2004-06-24	Antell et al.	
/J.J./	11	20040167984		2004-08-26	Herrmann	
/J.J./	12	20040193907		2004-09-30	Pantarella	
/J.J./	13	20040221174		2004-11-04	Le Saint et al.	
/J.J./	14	20050015622		2005-01-20	Williams et al.	
/J.J./	15	20050033596		2005-02-10	Tummolo	
/J.J./	16	20050044418		2005-02-24	Milliefsky	
/J.J./	17	20050060537		2005-03-17	Stamos et al.	
/J.J./	18	20050086511		2005-04-21	Balacheff et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	19	20050132225		2005-06-16	Gearhart	
/J.J./	20	20050138408		2005-06-23	Vanover et al.	
/J.J./	21	20050144475		2005-06-30	Sakaki et al.	
/J.J./	22	20050154885		2005-07-14	Viscomi et al.	
/J.J./	23	20050166065		2005-07-28	Eytchison et al.	
/J.J./	24	20050172142		2005-08-04	Shelest et al.	
/J.J./	25	20050188065		2005-08-25	O'Rourke et al.	
/J.J./	26	20050223221		2005-10-06	Proudlar et al.	
/J.J./	27	20050246767		2005-11-03	Fazal et al.	
/J.J./	28	20070124803		2007-05-31	Taraz	
/J.J./	29	20070143851		2007-06-21	Nicodemus et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	30	20070143827		2007-06-21	Nicodemus et al.	
--------	----	-------------	--	------------	------------------	--

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS

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 ⁶
/J.J./	1	Introduction to Radius, Radius - GNU Project - Free Software Foundation (FSF), 5 pages.	☐
/J.J./	2	Overview 1, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
/J.J./	3	Overview 2, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
/J.J./	4	Security Solutions that are Persistent and Pervasive...Yet Transparent to the End User, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
/J.J./	5	Virtual Private Networking in Windows 2000: An Overview, Microsoft Windows 2000 Server (1999) 28 pages.	☐

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	6	Wi-Fi Security at Work and on the Road, 5 pages.	☐
/J.J./	7	DAVIES, Joseph, Radius Protocol Security and Best Practices, Microsoft Windows 2000 Server (January 2002), 16 pages.	☐
/J.J./	8	TYSON, Jeff, How Virtual Private Networks Work, Howstuffworks, (07/12/2005), 10 pages.	☐
/J.J./	9	Novell eDirectory 8.7 Quick Look, http://www.novell.com/products/edirectory/quicklook.html , 2 pages.	☐
/J.J./	10	Novell eDirectory, Directory Services, Technical White Paper, www.novell.com , 23 pages.	☐
/J.J./	11	Novell Secure Login Features and Benefits, http://www.novell.com/products/securelogin/features.html , 2 pages.	☐
/J.J./	12	Novell Secure Login Quick Look, http://www.novell.com/products/securelogin/quicklook.html , 2 pages.	☐
/J.J./	13	International Search Report dated February 6, 2008 from PCT/US06/048720	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Josnel Jeudy/	Date Considered	02/23/2014
--------------------	----------------	-----------------	------------

*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 precode 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.

Search Notes 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 67/1012, H04L 29/08189	02/21/2014	JJ

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
H04L 63/20, H04L 63/10, H04L 29/08	02/21/2014	JJ

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	22-30	02/21/2014	JJ

SEARCH NOTES		
Search Notes	Date	Examiner
726/22-30 combined with computer, workstation, endpoint, compliance, compliant, monitor, state, condition, access, resource, data, content	2/21/2014	JJ
East, Google	2/21/2014	JJ

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/JOSNEL JEUDY/
Examiner, Art Unit 2438

<i>Index of Claims</i> 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA				☐ T.D.				☐ R.1.47			
CLAIM			DATE												
Final	Original	02/23/2014													
	1	-													
	2	-													
	3	-													
	4	-													
	5	-													
	6	-													
	7	-													
	8	-													
	9	-													
	10	-													
	11	-													
	12	-													
	13	-													
	14	-													
	15	-													
	16	-													
	17	-													
	18	-													
	19	-													
	20	-													
	21	-													
	22	-													
	23	-													
	24	-													
	25	-													
	26	-													
	27	-													
	28	-													
	29	-													
	30	-													
	31	✓													
	32	✓													
	33	✓													
	34	✓													
	35	✓													
	36	✓													

<i>Index of Claims</i> 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA				☐ T.D.				☐ R.1.47			
CLAIM			DATE												
Final	Original	02/23/2014													
	37	✓													
	38	✓													
	39	✓													
	40	✓													
	41	✓													
	42	✓													
	43	✓													
	44	✓													
	45	✓													
	46	✓													
	47	✓													
	48	✓													
	49	✓													
	50	✓													
	51	✓													
	52	✓													
	53	✓													
	54	✓													
	55	✓													
	56	✓													
	57	✓													
	58	✓													
	59	✓													
	60	✓													
	61	✓													
	62	✓													
	63	✓													



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9471

SERIAL NUMBER 13/587,505	FILING or 371(c) DATE 08/16/2012 RULE	CLASS 726	GROUP ART UNIT 2438	ATTORNEY DOCKET NO. 130839.00921		
APPLICANTS INVENTORS Blair Nicodemus, North Wales, PA; Billy Edison Stephens, West Chester, PA; ** CONTINUING DATA ***** This application is a CON of 11/451,950 06/13/2006 ABN which claims benefit of 60/752,424 12/21/2005 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ** 08/27/2012						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a) conditions met ☐ Yes ☒ No Verified and Acknowledged <u>JOSNIE J. FLOYD</u> Examiner's Signature		☐ Met after Allowance <u>Incis</u>	STATE OR COUNTRY PA	SHEETS DRAWINGS 7	TOTAL CLAIMS 33	INDEPENDENT CLAIMS 3
ADDRESS Pepper Hamilton LLP 400 Berywn Park 899 Cassatt Road Berwyn, PA 19312-1183 UNITED STATES						
TITLE METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES						
FILING FEE RECEIVED 1320	FEES: Authority has been given in Paper No. to charge/credit DEPOSIT ACCOUNT No. for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other ☐ Credit		

DOCKET NO.: 130839.00921
Application No.: 13/587,505
Response to Office Action dated: March 4, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Blair Nicodemus et al.**

**Title: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO
COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES**

Application No.: **13/587,505**

Group Art Unit: **2438**

Filed: **August 16, 2012**

Examiner: **Josnel Jeudy**

Confirmation No.: **9471**

Filed by EFS on: **June 4, 2014**

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

**AMENDMENT AND REQUEST FOR
RECONSIDERATION UNDER 35 U.S.C. § 1.111**

Sir:

In response to the Office Action mailed on March 4, 2014, Applicants respectfully request reconsideration in light of the:

Listing of the Claims, reflecting current amendments, beginning on page 2; and

Remarks beginning on page 7 of this paper.

Listing of Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

1-30. (Canceled)

31. (Presently Amended) A method for controlling the operation of an endpoint, comprising:

providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;

maintaining the plurality of policies in a data store on the computing system;

identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor;

configuring one or more software agents on the endpoint to monitor the plurality of conditions;

receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more software agents;

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and

initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

32. (Previously Presented) The method of claim 31, wherein the action comprises controlling access of the endpoint to computing resources.

33. (Previously Presented) The method of claim 31, wherein the user interface comprises a web page.

34. (Previously Presented) The method of claim 31, further comprising requesting, at the computing system, the status information on a periodic basis.

35. (Previously Presented) The method of claim 31, wherein the endpoint comprises a mobile device.

36. (Presently Amended) The method of claim 31, wherein the ~~plurality of one or more software~~ agents comprise at least one service provided by the operating system of the endpoint.

37. (Presently Amended) The method of claim 31, wherein the ~~plurality of one or more software~~ agents comprise at least one application running on the endpoint.

38. (Previously Presented) The method of claim 31, wherein the conditions comprise at least one hardware condition.

39. (Previously Presented) The method of claim 31, wherein the conditions comprise at least one software condition.

40. (Previously Presented) The method of claim 31, wherein the computing system comprises a plurality of servers.

41. (Previously Presented) The method of claim 31, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.

42. (Presently Amended) A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising:
providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;
maintaining the plurality of policies in a data store on the computing system;
identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor;
configuring one or more software agents on the endpoint to monitor the plurality of conditions;

receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more software agents;
determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and
initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

43. (Previously Presented) The computer readable medium of claim 42, wherein the action comprises controlling access of the endpoint to computing resources.

44. (Previously Presented) The computer readable medium of claim 42, wherein the user interface comprises a web page.

45. (Previously Presented) The computer readable medium of claim 42, further comprising requesting, at the computing system, the status information on a periodic basis.

46. (Previously Presented) The computer readable medium of claim 42, wherein the endpoint comprises a mobile device.

47. (Presently Amended) The computer readable medium of claim 42, wherein the ~~plurality of~~ one or more software agents comprise at least one service provided by the operating system of the endpoint.

48. (Presently Amended) The computer readable medium of claim 42, wherein the ~~plurality of~~ one or more software agents comprise at least one application running on the endpoint.

49. (Previously Presented) The computer readable medium of claim 42, wherein the conditions comprise at least one hardware condition.

50. (Previously Presented) The computer readable medium of claim 42, wherein the conditions comprise at least one software condition.

51. (Previously Presented) The computer readable medium of claim 42, wherein the computing system comprises a plurality of servers.

52. (Previously Presented) The computer readable medium of claim 42, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.

53. (Presently Amended) A system for controlling the operation of an endpoint, comprising:

- a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;

- a data store, at the computing system, that contains the plurality of policies;

- one or more software agents on the endpoint configured to monitor a plurality of conditions identified in the plurality of policies; and

- one or more processors at the computing system configured to:

- receive, across a network, status information about the plurality of conditions on the endpoint gathered by the one or more software agents,

- determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and

- initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

54. (Previously Presented) The system of claim 53, wherein the action comprises controlling access of the endpoint to computing resources.

55. (Previously Presented) The system of claim 53, wherein the user interface comprises a web page.

56. (Previously Presented) The system of claim 53, wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis.

57. (Previously Presented) The system of claim 53, wherein the endpoint comprises a mobile device.

58. (Presently Amended) The system of claim 53, wherein the ~~plurality of one or more software~~ agents comprise at least one service provided by the operating system of the endpoint.

59. (Presently Amended) The system of claim 53, wherein the ~~plurality of one or more software~~ agents comprise at least one application running on the endpoint.

60. (Previously Presented) The system of claim 53, wherein the conditions comprise at least one hardware condition.

61. (Previously Presented) The system of claim 53, wherein the conditions comprise at least one software condition.

62. (Previously Presented) The system of claim 53, wherein the computing system comprises a plurality of servers.

63. (Previously Presented) The system of claim 53, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.

REMARKS

Claims 31-63 were pending in the application. Claims 1-30 have been previously withdrawn from consideration. Claims 31, 36, 37, 42, 47, 48, 53, 58, and 59 have been amended. Support for these amendments can be found throughout the application, including but not limited to paragraphs 97-361, 639, 654-725, 1138-1119 (of the printed publication). No new matter has been introduced. Accordingly, upon entry of this amendment, claims 31-63 remain before the Examiner.

Rejections Under 35 U.S.C. § 101

Claims 53-63 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Applicants respectfully note that claim 53 recites “one or more processors at the computing system configured to...” Accordingly, the claim recites a specific machine specially adapted to carry out the recited functions. Accordingly, claim 53 and its dependent claims recite sufficient structure to comply the machine or transformation test that was endorsed by the Supreme Court in *Bilski*. *Bilski v. Kappos*, 130 S. Ct. 3218; 177 L. Ed. 2d 792 (2010). Accordingly, Applicants respectfully request withdrawal of this rejection.

Rejections Under 35 U.S.C. § 102

Claims 31-33, 36-39, 41-44, 47-50, 52-55, 58-61, and 63 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Balacheff et al. (U.S. Patent Publication No. 2005/0086511).

While the Examiner alleges that each element is taught in Balacheff, Applicants respectfully disagree with the alleged scope of the teaching of the Balacheff reference. Reading Balacheff in context, it becomes clear why Balacheff fails to teach the recited elements. Namely, Balacheff relates to a “method of and apparatus for controlling access to data.” Balacheff, Title. To that end, a “first data processing device performs the steps of: 1) obtaining information about the ability of the second data processing device to respect and uphold conditions specified in the first policy, and 2) an evaluation step where on a basis of a comparison between the first policy and the ability of the second data processing device to respect and uphold the first policy, the first data processing device decides whether to allow the operation to be performed.” Balacheff at [0004]. “In this context this means that they

will respect any restrictions imposed on the use of the data by an owner of the data. Thus trusted networks can be defined on a peer-to-peer basis.” *Id.* at [0005]. With this context in mind, it would be understood by a person having ordinary skill in the art that Balacheff teaches a system that uses policies in a different manner than claimed by the present invention.

Namely, Balacheff teaches rules for defining the trusted status that another computer must have before receiving access by a remote system. *See, e.g.*, Balacheff, FIG. 2. Balacheff’s rules are directed to ensuring that devices have trusted status before granting network access to the devices; Balacheff is not concerned with managing endpoints remotely. Instead, Balacheff teaches testing compliance of a device attempting to remotely access information, *inter alia*, by requesting information about the compliance status / integrity of the device from a trusted hardware component within the device seeking access. *See, e.g.*, Balacheff at [0044]. This trusted hardware component is a specific hardware device designed to create this integrity metric before the BIOS runs on startup of that device. *Id.* at [0042]. Applicants understand this trusted hardware component to be the alleged agent in the Office Action.

As a preliminary matter, the independent claims have been amended to state that the claimed agent is a software agent, which Applicants respectfully submit distinguishes the alleged agent of Balacheff. Furthermore, to the extent that hardware operates with software, Balacheff fails to teach the specific features of the claimed software agents. For example, Claim 31 recites “identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor” and “configuring one or more software agents on the endpoint to monitor the plurality of conditions.” In contrast, the integrity metrics and logs of Balacheff are not taught as configurable, nor does Balacheff teach that the conditions monitored to create an integrity metric are configurable or are identified from the plurality of policies. *See, e.g.*, Balacheff at [0042-44]. Rather than teaching configurable software agents that assist in controlling the operation of endpoints, Balacheff teaches sending logs or integrity metrics upon request.

The amended claims also recite, for example, that “the action is carried out by a processor on the endpoint.” In contrast, the identified actions in Balacheff are taken at the host, such as granting or denying access. *See, e.g.*, Balacheff at [0047-51], Fig. 2.

For at least these reasons, Applicants respectfully submit that independent claims 31, 42, and 53 are allowable as novel and non-obvious over Balacheff. The remaining dependent claims are similarly allowable because they depend from claims that are novel over the prior art.

Rejections Under 35 U.S.C. § 103

Claims 34, 35, 45, 46, 56, and 57 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Balacheff et al. in view of Newstadt et al. (U.S. Patent No. 7,805,752).

Claims 40, 51, and 62 are rejected stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Balacheff et al. in view of Taraz (U.S. Patent Publication No. 2007/0124803).

Applicants submit that neither Newstadt nor Taraz cure any of the deficiencies discussed above with respect to the teachings of Balacheff.

Furthermore, because each of these claims depend from and incorporate all of the limitations of the respective independent claims, these dependent claims are non-obvious over the cited references for at least the reasons stated above with respect to the independent claims. See MPEP §2143.03 (stating that if an independent claim is nonobvious under 35 U.S.C. §103, then any claim depending therefrom is nonobvious). Applicants also believe that any further discussion of the patentability of the additional elements in the dependent claims in light of infirmities of the prior art is not needed as moot. However, Applicants reserve the right to discuss these individual elements further if the Examiner disagrees with Applicants current arguments with respect to the independent claim.

Accordingly, Applicants respectfully request that the rejections associated with these remaining claims be withdrawn and allowance of these claims be swiftly granted.

DOCKET NO.: 130839.00921
Application No.: 13/587,505
Response to Office Action dated: March 4, 2014

CONCLUSION

Early reconsideration and allowance of all pending claims is respectfully requested. The Examiner is requested to contact the undersigned attorney if an interview, telephonic or personal, would facilitate allowance of the claims.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this response, or credit any overpayment, to deposit account no. 50-0436.

Respectfully Submitted

By: /Jay R. Mitchell, Reg. No. 54316/
Jay R. Mitchell
Registration No. 54,316

Dated: **June 4, 2014**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4664
Facsimile: (610) 640-7835

Electronic Acknowledgement Receipt	
EFS ID:	19211024
Application Number:	13587505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair Nicodemus
Customer Number:	86308
Filer:	Jay R. Mitchell/Sara Harvell
Filer Authorized By:	Jay R. Mitchell
Attorney Docket Number:	130839.00921
Receipt Date:	04-JUN-2014
Filing Date:	16-AUG-2012
Time Stamp:	15:45:00
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		921Response.pdf	121510	yes	10
			d: 004285d440c0e571381e750a251e4d91e30e091		

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	10
Warnings:			
Information:			
Total Files Size (in bytes):		121510	
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Document Number 13/587,505		Filing Date 08/16/2012		☐ To be Valid	
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO									
APPLICATION AS FILED – PART I									
(Column 1)		(Column 2)							
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)	
☐ BASIC FEE (37 CFR 1.16(a)(1)(i)-(iv))		N/A		N/A		N/A			
☐ SEARCH FEE (37 CFR 1.16(a)(1)(v)-(vi))		N/A		N/A		N/A			
☐ EXAMINATION FEE (37 CFR 1.16(a)(1)(vii)-(viii))		N/A		N/A		N/A			
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =		^		X \$		-	
INDEPENDENT CLAIMS (37 CFR 1.16(j))		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(i))									
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL			
APPLICATION AS AMENDED – PART II									
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	06/04/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	+ 33	Minus	= 33	= 0	X \$40 =		0	
	Independent (37 CFR 1.16(j))	+ 3	Minus	= 3	= 0	X \$210 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(i))								
TOTAL ADD'L FEE						0			
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	=	Minus	=	=	X \$		-	
	Independent (37 CFR 1.16(j))	=	Minus	=	=	X \$		-	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(i))								
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.									

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22315-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

86308 7250 08/28/2014
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

EXAMINER

JUDY, JOSNEL

ART UNIT

PAPER NUMBER

2438

DATE MAILED: 08/28/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921	9471

TITLE OF INVENTION: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES

APPL. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEES DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	11/28/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE, and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

86508 7550 08/28/2014
 Pepper Hamilton LLP
 400 Berywn Park
 899 Cassatt Road
 Berwyn, PA 19312-1183

Note: A certificate of mailing can only be used for domestic mailings of the fee(s) transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this fee(s) transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273 2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921	9471

TITLE OF INVENTION: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES

APPL. TYPE	ENTITY STATUS	ISSUE FEE DUL	PUBLICATION FEE DUL	PRIV. PAID ISSUE FEE	TOTAL FEE DUL	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	11/28/2014

EXAMINER	ART UNIT	CLASS SUBCLASS
IBUDY, JOSEPH	2438	/26-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47, Rev 03/02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1
 (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2
 3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
☐ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature

Date

Typed or printed name

Registration No.



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 22315-1450
www.uspto.gov

APPLICATION NO.	FILED DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921	9471
86308	7250	08/28/2014	EXAMINER	
Pepper Hamilton LLP 400 Berywn Park 899 Cassatt Road Berwyn, PA 19312-1183			JUDY, JOSNEL	
			ART UNIT	PAPER NUMBER
			2438	

DATE MAILED: 08/28/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND THESE OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/587,505	Applicant(s) NICODEMUS ET AL.	
	Examiner JOSNEL JEUDY	Art Unit 2438	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable. PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 06/04/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 31-63. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

<ol style="list-style-type: none"> 1. ☒ Notice of References Cited (PTO-892) 2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>11/11/2013</u> 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material 4. ☒ Interview Summary (PTO-413), Paper No./Mail Date <u>08/20/2014</u>. 	<ol style="list-style-type: none"> 5. ☒ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	---

/JOSNEL JEUDY/
Examiner, Art Unit 2438

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-30 have been cancelled.
4. Claims 31, 42 and 53 have been amended.
5. No claim has been added.
6. Claims 1-63 are re-numbered as claims 1-33 are pending.

Examiner's Amendment

7. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Jay R. Mitchell on August 20, 2014 to amend claims 31, 42 and 53.

The application has been amended as follows:

CLAIMS:

8. Please replace claims 31, 42 and 53 as follows:

31. (Presently Amended) A method for controlling the operation of an endpoint, comprising:
providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;
maintaining the plurality of policies in a data store on the computing system;
identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;

configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;

receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and

initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

42. (Presently Amended) A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising:

providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;

maintaining the plurality of policies in a data store on the computing system;

identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;

configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;

receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and

initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

53. (Presently Amended) A system for controlling the operation of an endpoint, comprising:

a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;

a data store, at the computing system, that contains the plurality of policies;

one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and

one or more hardware processors at the computing system configured to:

receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,

determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and

initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a the hardware processor on the endpoint.

Allowable Subject Matter

9. Claims 31, 42 and 53 are allowed. The following is an examiner's statement of reasons for allowance: Claims 31, 42 and 53 are allowed in view of the examiner's amendment and for reasons argued by applicant in pages 7-8 of the Remarks, filed on June 06, 2014, and dependent claims 32-41, 43-52 and 54-63 depend upon one of the above-mentioned allowed claims and are therefore allowed by virtue of their dependencies.

Balacheff (US 20050086511) prior art of record teaches providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;

maintaining the plurality of policies in a data store on the computing system;

The prior arts of record do not teach or suggest individually or in combination the limitation of independent claim 31 and similarly recited in independent claims 42 and 53:

identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor;

configuring one or more software agents on the endpoint to monitor the plurality of conditions;

receiving, across a network, at the computing system, status information about the plurality of conditions on the endpoint gathered by the one or more software agents;

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store;
and initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

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

Malik et al. US pat. No 20130007245.

Srinivasan et al. US pat. No 20110099255.

Gauvin et al. US Pat. No 8104077.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeudy Josnel whose telephone number is (571)270-7476. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number: 13/587,505
Art Unit: 2438

Page 6

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Date: 08/20/2014

/JOSNEL JEUDY/

Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 13/587,505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.	
	Examiner JOSNEL JEUDY	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2013/0007245	01-2013	MALIK et al.	709/223
*	B	US-2011/0099255	04-2011	Srinivasan et al.	709/221
*	C	US-8,104,077	01-2012	Gauvin et al.	726/12
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a))
Dates in MM-YYYY format are publication dates. Classifications may be U.S. or foreign.

<i>Index of Claims</i> 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA				☐ T.D.				☐ R.1.47			
CLAIM		DATE													
Final	Original	02/23/2014	08/21/2014												
	1	-	-												
	2	-	-												
	3	-	-												
	4	-	-												
	5	-	-												
	6	-	-												
	7	-	-												
	8	-	-												
	9	-	-												
	10	-	-												
	11	-	-												
	12	-	-												
	13	-	-												
	14	-	-												
	15	-	-												
	16	-	-												
	17	-	-												
	18	-	-												
	19	-	-												
	20	-	-												
	21	-	-												
	22	-	-												
	23	-	-												
	24	-	-												
	25	-	-												
	26	-	-												
	27	-	-												
	28	-	-												
	29	-	-												
	30	-	-												
1	31	✓	=												
2	32	✓	=												
3	33	✓	=												
4	34	✓	=												
5	35	✓	=												
6	36	✓	=												

<i>Index of Claims</i> 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA		☐ T.D.		☐ R.1.47	
CLAIM		DATE							
Final	Original	02/23/2014	08/21/2014						
7	37	✓	=						
8	38	✓	=						
9	39	✓	=						
10	40	✓	=						
11	41	✓	=						
12	42	✓	=						
13	43	✓	=						
14	44	✓	=						
15	45	✓	=						
16	46	✓	=						
17	47	✓	=						
18	48	✓	=						
19	49	✓	=						
20	50	✓	=						
21	51	✓	=						
22	52	✓	=						
23	53	✓	=						
24	54	✓	=						
25	55	✓	=						
26	56	✓	=						
27	57	✓	=						
28	58	✓	=						
29	59	✓	=						
30	60	✓	=						
31	61	✓	=						
32	62	✓	=						
33	63	✓	=						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1240	((config or config\$6 or format\$4) near (police\$3)) with (client or endpoint or terminal or client or enduser or device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:25
L2	14	((config or config\$6 or format\$4) near (police\$3)) with (client or endpoint or terminal or client or enduser or device) with (compliance or compliant)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:26
L3	2632	(client or endpoint or terminal or client or enduser or device) with (check\$3 or detect\$3 or determin\$5) with (status or condition) same (threat or virus or rogue or attack or vulnerab\$6 or risk)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:41
L4	34673	(726/1,7,17,21,25-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/21 13:41
L5	137	(client or endpoint or terminal or client or enduser or device) with (check\$3 or detect\$3 or determin\$5) with (status or condition) same (threat or virus or rogue or attack or vulnerab\$6 or risk) and L4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:41
L6	1	(client or endpoint or terminal or client or enduser or device) with (check\$3 or detect\$3 or determin\$5) with (status or condition) same (threat or virus or rogue or attack or vulnerab\$6 or risk) and L4 and L1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:42
L7	213	((config or config\$6 or format\$4) near (police\$3)) with (client or endpoint or terminal or client or enduser or device) and L4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:44
L8	396	(Nicodemus blair or stephens billy or	US-PGPUB;	NEAR	OFF	2014/08/21

		fiberlink communications corporation or horizon technology)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			13:50
L9	3	(Nicodemus blair or stephens billy or fiberlink communications corporation or horizon technology)and (conditions endpoint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 13:50
S1	34623	(726/1,7,17,21,25-30).OCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/20 15:46
S2	2748	(717/172-173).OCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/20 15:46
S3	10	(713/200).OCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/20 15:47
S4	14	(713/201).OCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/20 15:47
S6	0	((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	NEAR	OFF	2014/08/21 10:37

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S7	0	((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:39

		software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.				
S8	0	"s1" and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:40
S9	0	"s2" and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:41
S10	0	"s3" and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:41
S11	0	"s4" and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:42

8/ 21/ 2014 1:52:11 PM

Receipt date: 11/11/2013

13587505 - GAU: 2438

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

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		13587505
	Filing Date		2012-08-16
	First Named Inventor	Blair Nicodemus	
	Art Unit	2438	
	Examiner Name	Josnel Jeudy	
	Attorney Docket Number	130839.00921	

U.S.PATENTS						
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
/J.J./	1	5666411		1997-09-09	McCarty	
/J.J./	2	5673322		1997-09-30	Pepe et al.	
/J.J./	3	5732074		1998-03-24	Spaur et al.	
/J.J./	4	5987611		1999-11-16	Freund	
/J.J./	5	6012100		2000-01-04	Frailong et al.	
/J.J./	6	6061650		2000-05-09	Malkin et al.	
/J.J./	7	6081508		2000-06-27	West et al.	
/J.J./	8	6151628		2000-11-21	Xu et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	9	6185609		2001-02-06	Rangarajan et al.	
/J.J./	10	6253327		2001-06-26	Zhang et al.	
/J.J./	11	6298445		2001-10-02	Shostack et al.	
/J.J./	12	6377982		2002-04-23	Rai et al.	
/J.J./	13	6453035		2002-09-17	Psarras et al.	
/J.J./	14	6493349		2002-12-10	Casey	
/J.J./	15	6539482		2003-03-25	Blanco et al.	
/J.J./	16	6643782		2003-11-04	Jin et al.	
/J.J./	17	6654891		2003-11-25	Borsato et al.	
/J.J./	18	6694437		2004-02-17	Pao et al.	
/J.J./	19	6732270		2004-05-04	Patzer et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	20	6748543		2004-06-08	Vilhuber	
/J.J./	21	6751729		2004-06-15	Ginger et al.	
/J.J./	22	6760444		2004-07-06	Leung	
/J.J./	23	6766453		2004-07-20	Nessett et al.	
/J.J./	24	6778498		2004-08-17	McDysan	
/J.J./	25	6785823		2004-08-31	Abrol et al.	
/J.J./	26	6850943		2005-02-01	Teixeira et al.	
/J.J./	27	6874139		2005-03-29	Krueger et al.	
/J.J./	28	7058821		2006-06-06	Parekh et al.	
/J.J./	29	7185192		2007-02-27	Kahn	
/J.J./	30	7243148		2007-07-10	Keir et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	31	7673323		2010-03-02	Moriconi	
/J.J./	32	7805752		2010-09-28	Newstadt et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/J.J./	1	20020138756		2002-09-26	Makofka et al.	
/J.J./	2	20020199203		2002-12-26	Duffey et al.	
/J.J./	3	20030074580		2003-04-17	Knouse et al.	
/J.J./	4	20030105978		2003-06-05	Byrne	
/J.J./	5	20030135611		2003-07-17	Kemp et al.	
/J.J./	6	20030172292		2003-09-11	Judge	
/J.J./	7	20040005886		2004-01-08	Oda et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	8	20040088565		2004-05-06	Norman et al.	
/J.J./	9	20040107360		2004-06-03	Herrmann et al.	
/J.J./	10	20040123162		2004-06-24	Antell et al.	
/J.J./	11	20040167984		2004-08-26	Herrmann	
/J.J./	12	20040193907		2004-09-30	Pantarella	
/J.J./	13	20040221174		2004-11-04	Le Saint et al.	
/J.J./	14	20050015622		2005-01-20	Williams et al.	
/J.J./	15	20050033596		2005-02-10	Tummolo	
/J.J./	16	20050044418		2005-02-24	Milliesky	
/J.J./	17	20050060537		2005-03-17	Stamos et al.	
/J.J./	18	20050086511		2005-04-21	Balacheff et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	19	20050132225		2005-06-16	Gearhart	
/J.J./	20	20050138408		2005-06-23	Vanover et al.	
/J.J./	21	20050144475		2005-06-30	Sakaki et al.	
/J.J./	22	20050154885		2005-07-14	Viscomi et al.	
/J.J./	23	20050166065		2005-07-28	Eytchison et al.	
/J.J./	24	20050172142		2005-08-04	Shelest et al.	
/J.J./	25	20050188065		2005-08-25	O'Rourke et al.	
/J.J./	26	20050223221		2005-10-06	Proudlar et al.	
/J.J./	27	20050246767		2005-11-03	Fazal et al.	
/J.J./	28	20070124803		2007-05-31	Taraz	
/J.J./	29	20070143851		2007-06-21	Nicodemus et al.	

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
Attorney Docket Number		130839.00921		

/J.J./	30	20070143827		2007-06-21	Nicodemus et al.	
--------	----	-------------	--	------------	------------------	--

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	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							☐

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

NON-PATENT LITERATURE DOCUMENTS

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 ⁶
/J.J./	1	Introduction to Radius, Radius - GNU Project - Free Software Foundation (FSF), 5 pages.	☐
/J.J./	2	Overview 1, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
/J.J./	3	Overview 2, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
/J.J./	4	Security Solutions that are Persistent and Pervasive...Yet Transparent to the End User, Fiberlink: Secure Remote Access Systems and Secure Broadband Services, 07/12/2005, 2 pages.	☐
/J.J./	5	Virtual Private Networking in Windows 2000: An Overview, Microsoft Windows 2000 Server (1999) 28 pages.	☐

Receipt date: 11/11/2013 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13587505	13587505 - GAU: 2438
	Filing Date		2012-08-16	
	First Named Inventor	Blair Nicodemus		
	Art Unit	2438		
	Examiner Name	Josnel Jeudy		
	Attorney Docket Number	130839.00921		

/J.J./	6	Wi-Fi Security at Work and on the Road, 5 pages.	☐
/J.J./	7	DAVIES, Joseph, Radius Protocol Security and Best Practices, Microsoft Windows 2000 Server (January 2002), 16 pages.	☐
/J.J./	8	TYSON, Jeff, How Virtual Private Networks Work, Howstuffworks, (07/12/2005), 10 pages.	☐
/J.J./	9	Novell eDirectory 8.7 Quick Look, http://www.novell.com/products/edirectory/quicklook.html , 2 pages.	☐
/J.J./	10	Novell eDirectory, Directory Services, Technical White Paper, www.novell.com , 23 pages.	☐
/J.J./	11	Novell Secure Login Features and Benefits, http://www.novell.com/products/securelogin/features.html , 2 pages.	☐
/J.J./	12	Novell Secure Login Quick Look, http://www.novell.com/products/securelogin/quicklook.html , 2 pages.	☐
/J.J./	13	International Search Report dated February 6, 2008 from PCT/US06/048720	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Josnel Jeudy/	Date Considered	08/21/2014
--------------------	----------------	-----------------	------------

*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 precode 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.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9471

SERIAL NUMBER 13/587,505	FILING or 371(c) DATE 08/16/2012 RULE	CLASS 726	GROUP ART UNIT 2438	ATTORNEY DOCKET NO. 130839.00921		
APPLICANTS INVENTORS Blair Nicodemus, North Wales, PA; Billy Edison Stephens, West Chester, PA; ** CONTINUING DATA ***** This application is a CON of 11/451,950 06/13/2006 ABN which claims benefit of 60/752,424 12/21/2005 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ** 08/27/2012						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a) conditions met ☐ Yes ☒ No Verified and Acknowledged <u>JOSNIE J. FLOYD</u> Examiner's Signature		☐ Met after Allowance <u>Incis</u>	STATE OR COUNTRY PA	SHEETS DRAWINGS 7	TOTAL CLAIMS 33	INDEPENDENT CLAIMS 3
ADDRESS Pepper Hamilton LLP 400 Berywn Park 899 Cassatt Road Berwyn, PA 19312-1183 UNITED STATES						
TITLE METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES						
FILING FEE RECEIVED 1320	FEES: Authority has been given in Paper No. to charge/credit DEPOSIT ACCOUNT No. for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other ☐ Credit		

Search Notes 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 67/1012, H04L 29/08189	02/21/2014	JJ

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
H04L 63/20, H04L 63/10, H04L 29/08	02/21/2014	JJ

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	22-30	02/21/2014	JJ
726	1, 7, 17, 21, 25-30	8/21/2014	JJ
717	172-173	8/21/2014	JJ
713	200, 201	8/21/2014	JJ

SEARCH NOTES		
Search Notes	Date	Examiner
726/22-30 combined with computer, workstation, endpoint, compliance, compliant, monitor, state, condition, access, resource, data, content East, Google	2/21/2014	JJ
class 726/1, 7, 17, 21, 25-30 combined with client, endpoint, terminal, check, detect, status, condition, threat, virus, configure, policy	2/21/2014	JJ
NPL combined with class 726/1, 7, 17, 21, 25-30 combined with client, endpoint, terminal, check, detect, status, condition, threat, virus, configure, policy	8/21/2014	JJ
Assignee search, Inventor search	8/21/2014	JJ
East, Google	8/21/2014	JJ

INTERFERENCE SEARCH

/JOSNEL JEUDY/ Examiner.Art Unit 2438	
--	--

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	1, 7, 17, 21, 25-30 and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	08/21/2014	JJ
717	172-173 and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	08/21/2014	JJ
713	200, 201 and ((provid\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	08/21/2014	JJ

/JOSNEL JEUDY/
Examiner, Art Unit 2438

Issue Classification 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

US ORIGINAL CLASSIFICATION						INTERNATIONAL CLASSIFICATION													
CLASS		SUBCLASS				CLAIMED					NON-CLAIMED								
725		-				H	3	4	L	29 / 06 (2006.01.01)									
CROSS REFERENCE(S)																			
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																		
726	-	7	17	21	25														
726	26	27	28	29	30														
717	172	173																	
713	200	201																	

		Total Claims Allowed:	
(Assistant Examiner)	(Date)	33	
JOSNEL JEUDY/ Examiner, Art Unit 2438	08/21/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	31, 42, 53	Fig 1

Issue Classification 	Application/Control No. 13587505	Applicant(s)/Patent Under Reexamination NICODEMUS ET AL.
	Examiner JOSNEL JEUDY	Art Unit 2438

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	2		17	3	33	19	49								
	3		18	4	34	20	50								
			19	5	35	21	51								
	4		20	6	36	22	52								
	5		21	7	37	23	53								
	6		22	8	38	24	54								
	7		23	9	39	25	55								
	8		24	10	40	26	56								
	9		25	11	41	27	57								
	10		26	12	42	28	58								
	11		27	13	43	29	59								
	12		28	14	44	30	60								
	13		29	15	45	31	61								
	14		30	16	46	32	62								
	15		31	17	47	33	63								
	16	2	32	18	48										

		Total Claims Allowed:	
(Assistant Examiner)	(Date)	33	
JOSNEL JEUDY/ Examiner, Art Unit 2438	08/21/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	31, 42, 53	Fig 1

U.S. Patent and Trademark Office

Patent Paper No. 20140820

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	0	((provide\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:39
L3	0	"s1" and ((provide\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:40
L4	0	"s2" and ((provide\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:41
L5	0	"s3" and ((provide\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:41
L6	0	"s4" and ((provide\$3 user interface config\$5 allow\$3 config\$5 plurality polic\$3) with (maintain\$3 polic\$3 data store) with (identif\$3 plurality conditions endpoint monitor) with (config\$5 software agent endpoint monitor conditions)with(receiv\$3 status information conditions softare agents) with (determin\$3 compliance state endpoint based status information compliance polic\$3) with (initiat\$3 action identif\$3 rule)).clm.	US-PGPUB; USPAT; UPAD	NEAR	OFF	2014/08/21 10:42

8/21/2014 10:44:30 AM

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
 or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

80908 75506 08/20/2014
 Pepper Hamilton LLP
 400 Berywn Park
 809 Cassatt Road
 Berwyn, PA 19312-1183

Note: A certificate of mailing can only be used for domestic mailings of the fee(s) transmittal. This certificate cannot be used for any other accompanying papers, such as an assignment or Formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below:

Depositor's name:
Signature:
Date:

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921	9471

TITLE OF INVENTION: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES

APPL. TYPE	ENTITY STATUS	ISSUE FEE/DISC.	PUBLICATION FEE/DISC.	PREV. PAID ISSUE FEE	TOTAL FEE/DISC.	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	11/28/2014

EXAMINER	ART UNIT	CLASS SUBJECT CLASS
BRUDY, JOSEPH	2138	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication for "Fee Address" Indication form PTO/SB/47; Rev 03/02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR alternatively

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Pepper Hamilton LLP

2

3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE (CITY and STATE OR COUNTRY)

FIBERLINK COMMUNICATIONS CORPORATION

BLUE BELL, PENNSYLVANIA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☒ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 50-0436 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
☐ Applicant asserting small entity status. See 37 CFR 1.27
☒ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Michael K. Jones, Reg. #41100/

Date November 20, 2014

Typed or printed name Michael K. Jones

Registration No 41,100

DOCKET NO.: 130839.00921
Application No.: 13/587,505

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Blair Nicodemus et al.**

**Title: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO
COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES**

Application No.: **13/587,505**

Group Art Unit: **2438**

Filed: **August 16, 2012**

Examiner: **Josnel Jeudy**

Confirmation No.: **9471**

Filed by EFS on: **June 4, 2014**

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

**NOTIFICATION OF LOSS OF SMALL ENTITY STATUS
UNDER 37 C.F.R. §1.27(g)(2)**

Sir:

Notification under 37 C.F.R. §1.27(g)(2) is hereby given that small entity status is no longer appropriate for the above-identified application.

The Issue Fee is being paid concurrently herewith at the large entity rate.

Respectfully Submitted

By: /Michael K. Jones, Reg. No. 41100/
Michael K. Jones
Registration No. 41,100

Dated: **November 20, 2014**
PEPPER HAMILTON LLP
3000 Two Logan Square
Eighteenth and Arch Street
Philadelphia, PA 19103-279
Telephone: (215) 981-4405
Facsimile: (610) 640-7835

Electronic Patent Application Fee Transmittal				
Application Number:		13587505		
Filing Date:		16-Aug-2012		
Title of Invention:		METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES		
First Named Inventor/Applicant Name:		Blair Nicodemus		
Filer:		Michael Kenneth Jones/Sara Harvell		
Attorney Docket Number:		130839.00921		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				960

Electronic Acknowledgement Receipt	
EFS ID:	20756121
Application Number:	13587505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair Nicodemus
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.00921
Receipt Date:	20-NOV-2014
Filing Date:	16-AUG-2012
Time Stamp:	15:46:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 960
RAM confirmation Number	2271
Deposit Account	500436
Authorized User	JONES, MICHAEL K.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	921IssueFeeTransmittal.pdf	160258 / a1329500327169538173816e9edea274e7e5ed	no	1
Warnings:					
Information:					
2	Notification of loss of entitlement to small entity status	921LossSmallEntity.pdf	74729 / 7ed954d3d16e98857f1dce0e7a0845e0a38a	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30770 / 512920e4d9c7434c78a6e0a098230f4e1984	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1708086		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 450
Alexandria, Virginia 22304-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/587,505	02/10/2015	8955038	130839.00921	9471

85398 7590 01/21/2015
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Blair Nicodemus, North Wales, PA;
Billy Edison Stephens, West Chester, PA;

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 USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

**PATENT - POWER OF ATTORNEY
OR
REVOCATION OF POWER OF ATTORNEY
WITH A NEW POWER OF ATTORNEY
AND
CHANGE OF CORRESPONDENCE ADDRESS**

Patent Number	6 955 038
Issue Date	January 21, 2015
First Named Inventor	Blair Nicodemus
Title	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
Attorney Docket No.	AUS620145112US4

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ A Power of Attorney is submitted herewith.

OR I hereby appoint Practitioner(s) associated with the Customer Number identified in the box at right as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

26502

OR I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to:

☒ The address associated with the above-identified Customer Number.

OR

☐ The address associated with the Customer Number identified in the box at right:

OR

Print or

Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the:

☐ Inventor, having ownership of the patent.

OR

☒ Patent owner.

☒ Statement under 37 CFR 3.75(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of inventor or Patent Owner

Signature

Date

Name

Tuesday 4 April 2015, 10:37 AM

04/04/2015

Telephone

(703) 261-1156

Title and Company

Council, Information Systems Machine Corporation

NOTE: Signatures of all the inventors or patent owners of the entire interest or their representatives are required. If more than one signature is required, submit multiple forms. Check the box below, and identify the total number of forms submitted in the blank below.

☒ A total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.51, 1.52, and 1.53. The information is required to obtain or obtain a benefit by the public, which is to assist (and by the USPTO to protect) the file of a patent or request for prosecution. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 15 minutes to complete, including gathering, organizing, 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 22315-1450. DO NOT SEND THIS OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22315-1450.

If you need assistance in completing the form, call 1-800-PTO-5198 and select option 3.

Electronic Acknowledgement Receipt	
EFS ID:	3298//12
Application Number:	1358/505
International Application Number:	
Confirmation Number:	9471
Title of Invention:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES
First Named Inventor/Applicant Name:	Blair Nicodemus
Customer Number:	86308
Filer:	Michael Kenneth Jones/Sara Harvell
Filer Authorized By:	Michael Kenneth Jones
Attorney Docket Number:	130839.00921
Receipt Date:	25-JUN-2018
Filing Date:	16 AUG 2012
Time Stamp:	10:34:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no				
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	921Statement.pdf	314941 61244C3185c018e2285d02a51281031128 VRT	no	1
Warnings:					

Information:					
2	Power of Attorney	921POAIBM.pdf	285477	no	1
			e"dw71cGctt3*7z6796ct 9/2za3d9'00a8w rv'c9		
Warnings:					
Information:					
Total Files Size (in bytes):				600418	
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>					

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: International Business Machines Corporation

Application No./Patent No.: 8,955,038

Filed/Issue Date: February 10, 2015

Titled: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES

International Business Machines Corporation, a corporation

Name of Assignee:

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made) the patent application/patent identified above, by virtue of either:

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

OR

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

1. From: Blair Nicodemus; Billy E. Stephens To: Fiberlink Communications Corporation

The document was recorded in the United States Patent and Trademark Office at
Reel 031550, Frame 0640, or for which a copy thereof is attached.

2. From: Fiberlink Communications Corporation To: International Business Machines Corporation

The document was recorded in the United States Patent and Trademark Office at
Reel 039001, Frame 0462, or for which a copy thereof is attached.

3. From: _____ To: _____

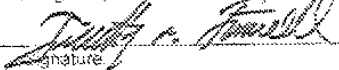
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.06]

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


Signature

June 20, 2018

Date

Timothy M. Farrell, USPTO Reg. No. 37,321

Counsel

Printed or Typed Name

Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public whom it is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 132 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comment 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-0199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: 400 M STREET, N.E., 10TH FLOOR
WASHINGTON, D.C. 20530
www.uspto.gov

APPLICATION NUMBER	FILING OR EFFECT DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./FILE NO.
13/587,505	08/16/2012	Blair Nicodemus	130839.00921

CONFIRMATION NO. 9471

POWER OF ATTORNEY NOTICE



OC000000100704595

86308
Pepper Hamilton LLP
400 Berywn Park
899 Cassatt Road
Berwyn, PA 19312-1183

Date Mailed: 07/10/2018

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/25/2018.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/qtran/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: 1515 M Street, NW, 4TH FLOOR
WASHINGTON, DC 20540
Alexandria, Virginia 22314-1150
www.uspto.gov

APPLICATION NUMBER	FILING OR PRIORITY DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./FILE NO.
13/587,505	08/16/2012	Blair Nicodemus	AUS920145112US4

CONFIRMATION NO. 9471

POA ACCEPTANCE LETTER



OC000000100704625

26502
IBM CORPORATION
IPLAW SHCB/256-3
1701 NORTH STREET
ENDICOTT, NY 13760

Date Mailed: 07/10/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/25/2018.

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.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/qtran/

AO 120 (Rev. 08/16)

Mail Stop 8 TO: Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292);

DOCKET NO. 2:21-cv-00441	DATE FILED 11/30/2021	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT TREND MICRO INCORPORATED
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,327,441	12/4/2012	Taasera Licensing LLC
4 8,850,517	9/30/2014	Taasera Licensing LLC
5 8,955,038	2/10/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

PAGE 1 of 2

AO 120 (Rev. 08/16)

Mail Stop 8 TO: Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292):

DOCKET NO. 2:21-cv-00441	DATE FILED 11/30/2021	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT TREND MICRO INCORPORATED
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,990,948	3/24/2015	Taasera Licensing LLC
2 9,092,616	7/28/2015	Taasera Licensing LLC
3 9,608,997	3/28/2017	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court _____ for the Eastern District of Texas, Marshall Division _____ on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:21-cv-00441	DATE FILED 11/30/2021	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT TREND MICRO INCORPORATED
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,327,441	12/4/2012	Taasera Licensing LLC
4 8,850,517	9/30/2014	Taasera Licensing LLC
5 8,955,038	2/10/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

PAGE 1 of 2

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:21-cv-00441	DATE FILED 11/30/2021	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT TREND MICRO INCORPORATED
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,990,948	3/24/2015	Taasera Licensing LLC
2 9,092,616	7/28/2015	Taasera Licensing LLC
3 9,608,997	3/28/2017	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

PAGE 2 of 2

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-00062	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT PALO ALTO NETWORKS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,127,356	2/28/2012	Taasera Licensing LLC
4 8,327,441	12/4/2012	Taasera Licensing LLC
5 8,850,517	9/30/2014	Taasera Licensing LLC

In the above entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY		
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 2:22-cv-00062	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT PALO ALTO NETWORKS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,955,038	2/10/2015	Taasera Licensing LLC
2 8,990,948	3/24/2015	Taasera Licensing LLC
3 9,092,616	7/28/2015	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 100 (Rev. 08/19)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 35 U.S.C. § 1116 you are hereby advised that a court action has been
 filed in the U.S. District Court **for the Eastern District of Texas, Marshall Division** on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.)

DOCKET NO. 2:22-cv-00063	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT CHECK POINT SOFTWARE TECHNOLOGIES LTD.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 8,327,441	12/4/2012	Taasera Licensing LLC
3 8,955,038	2/10/2015	Taasera Licensing LLC
4 8,990,948	3/24/2015	Taasera Licensing LLC
5 9,092,616	7/28/2015	Taasera Licensing LLC

In the above-captioned case, the following patent(s)/trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Assignment ☐ Answer ☐ Cross Petition ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above-captioned case, the following decision has been rendered or judgment issued:

DECISION/JUDGMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director. Copy 3—Upon termination of action, mail this copy to Director.
 Copy 2—Upon filing document adding patent(s), mail this copy to Director. Copy 4—Case file copy.

AO 100 (Rev. 08/19)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	--

In Compliance with 35 U.S.C. § 290 and/or 35 U.S.C. § 1116 you are hereby advised that a court action has been
 filed in the U.S. District Court **for the Eastern District of Texas, Marshall Division** on the following

☐ Trademarks or ☒ Patents (☐ the patent action involves 35 U.S.C. § 292.)

DOCKET NO. 2:22-cv-00063	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT CHECK POINT SOFTWARE TECHNOLOGIES LTD.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,608,997	3/28/2017	Taasera Licensing LLC
2 9,923,918	3/20/2018	Taasera Licensing LLC
3		
4		
5		

In the above-captioned case, the following patent(s)/trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Assignment ☐ Answer ☐ Cross Petition ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above-captioned case, the following decision has been rendered or judgment issued:

DECISION/JUDGMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director. Copy 3—Upon termination of action, mail this copy to Director.
 Copy 2—Upon filing document adding patent(s), mail this copy to Director. Copy 4—Case file copy.

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.)

DOCKET NO. 2:22-cv-00062	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT PALO ALTO NETWORKS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,842,796	1/11/2005	Taasera Licensing LLC
2 7,673,137	3/2/2010	Taasera Licensing LLC
3 8,127,356	2/28/2012	Taasera Licensing LLC
4 8,327,441	12/4/2012	Taasera Licensing LLC
5 8,850,517	9/30/2014	Taasera Licensing LLC

In the above entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08-10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. ☐ the patent action involves 35 U.S.C. § 292.)

DOCKET NO. 2:22-cv-00062	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT PALO ALTO NETWORKS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,955,038	2/10/2015	Taasera Licensing LLC
2 8,990,948	3/24/2015	Taasera Licensing LLC
3 9,092,616	7/28/2015	Taasera Licensing LLC
4 9,923,918	3/20/2018	Taasera Licensing LLC
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

Mail Stop 8 TO: Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-00063	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT CHECK POINT SOFTWARE TECHNOLOGIES LTD.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 8,327,441	12/4/2012	Taasera Licensing LLC
3 8,955,038	2/10/2015	Taasera Licensing LLC
4 8,990,948	3/24/2015	Taasera Licensing LLC
5 9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.)

DOCKET NO. 2:22-cv-00063	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT CHECK POINT SOFTWARE TECHNOLOGIES LTD.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,608,997	3/28/2017	Taasera Licensing LLC
2 9,923,918	3/20/2018	Taasera Licensing LLC
3		
4		
5		

In the above entitled case, the following patent(s) trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court _____ for the Eastern District of Texas, Marshall Division _____ on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-00063	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT CHECK POINT SOFTWARE TECHNOLOGIES LTD.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,842,796	1/11/2005	Taasera Licensing LLC
2 8,327,441	12/4/2012	Taasera Licensing LLC
3 8,955,038	2/10/2015	Taasera Licensing LLC
4 8,990,948	3/24/2015	Taasera Licensing LLC
5 9,092,616	7/28/2015	Taasera Licensing LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-00063	DATE FILED 2/25/2022	U.S. DISTRICT COURT for the Eastern District of Texas, Marshall Division
PLAINTIFF TAASERA LICENSING LLC		DEFENDANT CHECK POINT SOFTWARE TECHNOLOGIES LTD.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,608,997	3/28/2017	Taasera Licensing LLC
2 9,923,918	3/20/2018	Taasera Licensing LLC
3		
4		
5		

In the above-entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above-entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy