505909791 02/11/2020

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT5956508

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	RELEASE OF SECURITY INTEREST

CONVEYING PARTY DATA

Name	Execution Date
DLI LENDING AGENT, LLC	01/09/2020

RECEIVING PARTY DATA

Name:	CRYPTOPEAK SOLUTIONS, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106
Name:	ECTOLINK, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106
Name:	INTERFACE LINX, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106
Name:	SELECTIVE SIGNALS, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106
Name:	SI-FLASH DRIVES, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106
Name:	SOTERIA ENCRYPTION, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA

State/Country:	CALIFORNIA
Postal Code:	91106
Name:	SYNERGY DRONE, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106
Name:	UNIBEAM PHOTONICS, LLC
Street Address:	1055 E. COLORADO BLVD, SUITE 500
City:	PASADENA
State/Country:	CALIFORNIA
Postal Code:	91106

PROPERTY NUMBERS Total: 53

Property Type	Number
Patent Number:	6202150
Patent Number:	6243466
Patent Number:	6282295
Patent Number:	6389136
Patent Number:	5826245
Patent Number:	6508678
Patent Number:	8111629
Patent Number:	7855916
Patent Number:	8194452
Patent Number:	8531880
Patent Number:	8817537
Patent Number:	9257184
Patent Number:	7069447
Patent Number:	8200375
Patent Number:	8389368
Patent Number:	8649918
Patent Number:	9079116
Application Number:	14724037
Patent Number:	6075912
Patent Number:	7596570
Patent Number:	9201941
Application Number:	14953379
Patent Number:	8234705
Patent Number:	8149844

Property Type	Number
Patent Number:	7630381
Patent Number:	9516048
Patent Number:	9398037
Patent Number:	7712142
Patent Number:	8104092
Patent Number:	8645480
Patent Number:	8965892
Patent Number:	7092355
Patent Number:	6108642
Patent Number:	6714919
Patent Number:	7158947
Patent Number:	7657460
Patent Number:	8180687
Patent Number:	8682745
Patent Number:	6927727
Patent Number:	7394423
Patent Number:	7532157
Patent Number:	7746273
Application Number:	11488271
Patent Number:	8209437
Patent Number:	8539107
Patent Number:	7532890
Patent Number:	8428604
Patent Number:	9077673
Application Number:	13757775
Patent Number:	8881180
Patent Number:	9240964
Application Number:	14966903
Patent Number:	7523858

CORRESPONDENCE DATA

Fax Number: (212)586-5095

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 2125865800
Email: DFRIEDMAN@CTSWLAW.COM
Correspondent Name: DANIEL J. FRIEDMAN
Address Line 1: 420 LEXINGTON AVENUE
Address Line 2: SUITE 2400
Address Line 4: NEW YORK, NEW YORK 10170

NAME OF SUBMITTER:	DANIEL J. FRIEDMAN
SIGNATURE:	/Daniel J. Friedman/
DATE SIGNED:	02/11/2020
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 5
source=00410495#page1.tif
source=00410495#page2.tif
source=00410495#page3.tif
source=00410495#page4.tif
source=00410495#page5.tif

EXECUTION VERSION

NOTICE OF RELEASE OF
SECURITY INTEREST IN PATENTS

This NOTICE OF RELEASE OF SECURITY INTEREST IN PATENTS (this "Release"), effective as of January 9, 2020 is made by DLI LENDING AGENT, LLC (F/K/A BLACKBIRD FINANCIAL GROUP, LLC), in its capacity as collateral agent for the Credit Parties (in such capacity, the "Collateral Agent"), in favor of IPEL, INC., a Delaware limited liability company, ("Borrower"), , CRYPTOPEAK SOLUTIONS, LLC, a Texas limited liability company, ECTOLINK, LLC, a Texas limited liability company, INTERFACE LINX, LLC, a California limited liability company, SELECTIVE SIGNALS, LLC, a Texas limited liability company, SI-FLASH DRIVES, LLC, a California limited liability company, SOTERIA ENCRYPTION, LLC, a California limited liability company, SYNERGY DRONE LLC, , a Texas limited liability company, and UNIBEAM PHOTONICS, LLC, a Texas limited liability company, each with an address of 1055 E. Colorado Blvd., Suite 500, Pasadena, CA 91106 (each a "Releasee" and collectively, the "Releasees") .

W I T N E S S E T H:

WHEREAS, in connection with the Credit Agreement, dated as of May 5, 2017, among DLI ASSETS BRAVO, LLC ("Lender"), the Collateral Agent, ("Borrower") and the other parties thereto (the "Loan Agreement"), the Releasees executed and delivered the Intellectual Property Security Agreement, dated as of May 5, 2017, in favor of the Collateral Agent (the "Patent Security Agreement");

WHEREAS, pursuant to the Patent Security Agreement, the Releasees pledged and granted to the Collateral Agent a lien on and continuing security interest in all of the patents set forth on Schedule A attached hereto, together with all goodwill associated with such Patents (the "Released Patents");

WHEREAS, the Collateral Agent recorded its security interest in the Released Patents with the United States Patent and Trademark Office (the "USPTO") on May 23, 2017 at Reel 042554, Frame 0298; and

WHEREAS, the Lender and Collateral agent have duly authorized the execution, delivery and performance of this Release.

NOW THEREFORE, for good and valuable consideration, the receipt of which is hereby acknowledged, the Collateral Agent agrees, for the benefit of the Releasees, as follows:

SECTION 1. Definitions. Unless otherwise defined herein or the context otherwise requires, terms used in this Release, including its preamble and recitals, have the meanings provided or provided by reference in the Loan Agreement or Patent Security Agreement, as applicable.

SECTION 2. Release of Security Interest. The Collateral Agent does hereby release, relinquish and discharge its lien on and security interest in, and right of setoff against, all of the Releasees' right, title and interest in, to and under the Released Patents.

DocuSign Envelope ID: F2BBD4F1-F8C8-45C9-8DC6-7E710AECAFF5

SECTION 3. Choice of Law. This Release shall be governed by, and construed in accordance with, the laws of the State of California.

[Signatures Follow on Next Page.]

IN WITNESS WHEREOF, the Collateral Agent has caused this Notice of Release of Security Interest in Patents to be duly executed and delivered by its officer thereunto duly authorized as of the date set forth above.

DLI LENDING AGENT, LLC
as Collateral Agent

DocuSigned by:
By: Bradley Sharp
FEDFF3D4B8C445C...
Name: Bradley Sharp
Title: Receiver

SCHEDULE A

Patents

Portfolio #	Patent Asset Number	Portfolio Name	Portfolio Owner
1	6,202,150	CryptoPeak Solutions, LLC	
	6,243,466		CryptoPeak Solutions, LLC
	6,282,295		
	6,389,136		
2	5,826,245	EctoLink, LLC	EctoLink, LLC
3	6,508,678	Interface Linx, LLC	Interface Linx, LLC
4	8,111,629	Selective Signals, LLC	Selective Signals, LLC
5	7,855,916	Si-Flash Drives, LLC	
	8,194,452		
	8,531,880		Si-Flash Drives, LLC
	8,817,537		
	9,257,184		
6	7,069,447	Soteria Encryption, LLC	Soteria Encryption, LLC
7	8,200,375	Synergy Drone, LLC	
	8,389,368		
	8,649,918		Synergy Drone, LLC
	9,079,116		
	App. 14/724,037		
8	6,075,912	Unibeam Photonics, LLC	Unibeam Photonics, LLC
9	7,596,570	Data Backup	
	9,201,941		Spectrum Patents, Inc.
	App. 14/953,379		
10	8,234,705	Network Security	
	8,149,844		
	7,630,381		Spectrum Patents, Inc.
	9,516,048		
	9,398,037		
11	7,712,142	Data Security	
	8,104,092		Spectrum Patents, Inc.
	8,645,480		
	8,966,892		
12	7,092,355	Network Congestion	Spectrum Patents, Inc.
13	6,108,642	Fraud Detection	
	6,714,919		
	7,158,947		Spectrum Patents, Inc.
	7,657,460		
	8,180,697		
	8,682,745		
14	6,927,727	IP911	
	7,394,423		
	7,532,157		Spectrum Patents, Inc.

Portfolio #	Patent Asset Number	Portfolio Name	Portfolio Owner
	7,746,273		
	App. 11/488,271		
15	8,209,437	Rockliffe	
	8,599,107		
	7,532,890		Spectrum Patents, Inc.
	8,428,604		
	9,077,673		
	App. 13/757,775		
16	8,881,180	Jargon	
	9,240,964		Spectrum Patents, Inc.
	App. 14/966,903		
17	7,523,858	Secure Transactions	Spectrum Patents, Inc.

505861362 01/13/2020

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT5908299

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
NETWORK SECURITY TECHNOLOGIES, LLC	12/24/2019

RECEIVING PARTY DATA

Name:	K.MIZRA LLC
Street Address:	2160 CENTURY PARK EAST
Internal Address:	#707
City:	LOS ANGELES
State/Country:	CALIFORNIA
Postal Code:	90067

PROPERTY NUMBERS Total: 5

Property Type	Number
Patent Number:	8234705
Patent Number:	9398037
Patent Number:	7630381
Patent Number:	8149844
Patent Number:	9516048

CORRESPONDENCE DATA

Fax Number: (212)586-5095

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 2125865800
Email: DFRIEDMAN@CTSWLAW.COM
Correspondent Name: DANIEL J. FRIEDMAN
Address Line 1: 420 LEXINGTON AVENUE
Address Line 2: SUITE 2400
Address Line 4: NEW YORK, NEW YORK 10170

NAME OF SUBMITTER:	DANIEL J. FRIEDMAN
SIGNATURE:	/Daniel J. Friedman/
DATE SIGNED:	01/13/2020
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 2
source=00407807#page1.tif
source=00407807#page2.tif

ASSIGNMENT OF PATENTS AND PATENT RIGHTS

This ASSIGNMENT OF PATENTS AND PATENT RIGHTS (the "Assignment") is executed, acknowledged and delivered by Network Security Technologies, LLC, a Delaware limited liability company ("Assignor").

NOW, THEREFORE, TO ALL WHOM IT MAY CONCERN:

For good and valuable consideration, the receipt of which is hereby acknowledged, Assignor agrees to and does hereby irrevocably sell, assign, transfer, and convey unto K.Mizra LLC, a Delaware limited liability company, with its principal place of business at 2160 Century Park East # 707, Los Angeles, CA 90067 ("Assignee"), and Assignee hereby accepts, all of Assignor's right, title, and interest (i) in and to the patents and patent rights set forth on Exhibit 1 hereto (the "Patents"), together with the goodwill associated therewith, the same to be held and enjoyed by said Assignee for its own use, and for the use of its successors, assigns, or other legal representatives to the end of the term or terms for which said Patents may be granted as fully and entirely as the same would have been held and enjoyed by Assignor if this Assignment had not been made; and (ii) in and to any and all causes of action and enforcement rights for the Patents including, without limitation, all rights to pursue damages, injunctive relief and other remedies for past and future infringement of the Patents.

This Assignment shall be binding upon and shall inure to the benefit of the parties and their respective successors and assigns.

Assignee is hereby authorized to file or record this Assignment or any other instrument in such public offices and with such governmental authorities, including, without limitation, the United States Patent and Trademark Office, as Assignee may determine from time to time for the purpose of evidencing the foregoing assignment.

This Assignment shall be governed by, and construed in accordance with, the laws of the United States in respect to patent issues and in all other respects by the laws of the State of New York, without giving effect to the conflict of laws rules thereof.

IN WITNESS WHEREOF, Assignor has caused this Assignment to be executed as of this 24th day of December 2019.

Network Security Technologies, LLC

DocuSigned by:
By: _____
DAAEA6F409B34F9...
Name: Brian Yates
Title: CEO

EXHIBIT 1
Patents

Owner	Country	Application No.	Patent No.
Network Security Technologies, LLC	United States	11/237,003	8234705
Network Security Technologies, LLC	United States	11/237,004	9398037
Network Security Technologies, LLC	United States	11/237,199	7630381
Network Security Technologies, LLC	United States	12/605,338	8149844
Network Security Technologies, LLC	United States	15/206,227	9516048

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/237,003	09/27/2005	James A. Roskind	GLIA-030US-1

CONFIRMATION NO. 5151

98618
BrainSpark Associates, LLC
528 South Meadows Drive
Chandler, AZ 85224

POA ACCEPTANCE LETTER

"OC000000101710544"

Date Mailed: 08/15/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/09/2018.

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**.

/deelliott/

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/237,003	09/27/2005	James A. Roskind	PB-034

CONFIRMATION NO. 5151

POWER OF ATTORNEY NOTICE

85853
Aaron Emigh
762 Judith Court
Incline Village, NV 89451

OC000000101710419

Date Mailed: 08/15/2018

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/09/2018.

- 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**.

/deelliott/

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

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

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

Application Number	11/237,003
Filing Date	9-27-2005
First Named Inventor	James A. Roskind
Title	CONTAGION ISOLATION AND INOCULATION
Art Unit	2437
Examiner Name	SIMS, JING F
Attorney Docket Number	GLIA-030US-1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Joseph J. Basista/	Date (Optional)	
Name	Joseph J. Basista	Registration Number	42301
Title (if Applicant is a juristic entity)	Attorney of Record		
Applicant Name (if Applicant is a juristic entity)	NETWORK SECURITY TECHNOLOGIES, LLC		

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

☐ *Total of _____ forms are submitted.

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

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

GENERAL POWER OF ATTORNEY

	I/WE hereby appoint the practitioners associated with the Customer Number: **98618** with the firm: BRAINSPARK ASSOCIATES, LLC 528 S. Meadows Drive Chandler, AZ 85224 United States As attorneys to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications where the assignee is named as an applicant or where the applications are assigned to the undersigned according to the USPTO assignment records or assignment documents, in which case the details will be listed on an attached form in accordance with 37 C.F.R. 3.73(c).
	Address all correspondence to: **Customer Number 98618** Direct all Telephone Calls to: 650-924-9270 Direct all Facsimiles to: 480-535-9269 Direct all emails to: info@brainsparkassociates.com
Full Name and Registered Address of Assignee	Network Security Technologies, LLC 1055 E. Colorado Boulevard, Suite 500 Pasadena, CA 91106
The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).	
Date	Dated this 17th day of July 2018
Signature of Assignee	
Printed Name of Signatory	Katherine Huen
Title of Signatory	Chief Financial Officer

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: James A. Roskind

Application No./Patent No.: 11/237,003 Filed/Issue Date: 09-27-2005

Titled: CONTAGION ISOLATION AND INOCULATION

NETWORK SECURITY TECHNOLOGIES, LLC, a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

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

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

1. From: Inventors To: EMIGH, AARON

The document was recorded in the United States Patent and Trademark Office at
Reel 023388, Frame 0648, or for which a copy thereof is attached.

2. From: EMIGH, AARON To: RADIX HOLDINGS, LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 023388, Frame 0431, or for which a copy thereof is attached.

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

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

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: RADIX HOLDINGS, LLC To: SPECTRUM PATENTS, INC.

The document was recorded in the United States Patent and Trademark Office at
Reel 042311, Frame 0368, or for which a copy thereof is attached.

4. From: SPECTRUM PATENTS, INC. To: NETWORK SECURITY TECHNOLOGIES, LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 043862, Frame 0171, or for which a copy thereof is attached.

5. 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.

6. 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(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

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

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

/Joseph J. Basista/	9 August 2018
Signature	Date
Joseph J. Basista	42301
Printed or Typed Name	Title or Registration 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.

Electronic Acknowledgement Receipt

EFS ID:	33429137
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	CONTAGION ISOLATION AND INOCULATION
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Joseph John Basista
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	09-AUG-2018
Filing Date:	27-SEP-2005
Time Stamp:	19:51:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	GLIA-030US-1-Form82A-aia0082.pdf	181515 4b69c9e4823acb5185374b4b10d9e72cc1d12f5d	no	1

Warnings:

Information:					
2	Power of Attorney	GLIA-030US-GPOA-NetworkSecurityTechnologiesLLC-executed-embedded.pdf	143973 0cc68e0efb24fd8d4d41bd37dad60fffb3675171	no	1
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	GLIA-030US-1-373Statement-aia0096.pdf	122604 b1bea2f11ac40d60fa01871021956091fddb3adf	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	448092		

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.

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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	PULSE SECURE, LLC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	BRADFORD NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	MCAFEE, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	FORESCOUT TECHNOLOGIES, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	MCAFEE, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	PULSE SECURE, LLC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	BRADFORD NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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 District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
	10/24/2017	for the District of Delaware

PLAINTIFF	DEFENDANT
NETWORK SECURITY TECHNOLOGIES, LLC	FORESCOUT TECHNOLOGIES, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 8,234,705 B1	7/31/2012	Network Security Technologies, LLC
2	US 9,516,048 B1	12/6/2016	Network Security Technologies, 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**

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	07/31/2012	8234705	PB-034	5151

85853 7590 07/11/2012

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

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 1520 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):

James A. Roskind, Redwood City, CA;
Aaron T. Emigh, Incline Village, NV;

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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

85853 7590 06/21/2012
Aaron Emigh
762 Judith Court
Incline Village, NV 89451

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.

Aaron T. Emigh	(Depositor's name)
/Aaron T. Emigh/ (e-filed)	(Signature)
June 22, 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

TITLE OF INVENTION: CONTAGION ISOLATION AND INOCULATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	09/21/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
SIMS, JING F	2437	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Radix Holdings, LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Incline Village, Nevada

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 50-4831 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Aaron T. Emigh/ Date June 22, 2012

Typed or printed name Aaron T. Emigh Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

Electronic Patent Application Fee Transmittal

Application Number:	11237003
Filing Date:	27-Sep-2005
Title of Invention:	CONTAGION ISOLATION AND INOCULATION
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-034

Filed as Small 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	2501	1	870	870
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**870**

Electronic Acknowledgement Receipt

EFS ID:	13085426
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	CONTAGION ISOLATION AND INOCULATION
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	22-JUN-2012
Filing Date:	27-SEP-2005
Time Stamp:	15:57:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$870
RAM confirmation Number	2810
Deposit Account	504831
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	PB-034-issue-fee-printed.pdf	174381 6158e0fee095c2c6e5ac3fb[illegible]a530c3ecc4fae[illegible]11	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30017 b4[illegible]7ab7ae9fe5[illegible]4601b8[illegible]5e4e15b4e9965 3fe697	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	204398		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

85853 7590 06/21/2012

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER
SIMS, JING F

ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 06/21/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

TITLE OF INVENTION: CONTAGION ISOLATION AND INOCULATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	09/21/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

Ex.1002
NETSKOPE, INC. / Page 37 of 378

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

85853 7590 06/21/2012
Aaron Emigh
762 Judith Court
Incline Village, NV 89451

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

TITLE OF INVENTION: CONTAGION ISOLATION AND INOCULATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	09/21/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
SIMS, JING F	2437	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 06/21/2012

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	

ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 06/21/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 384 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 384 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

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.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

-- 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 *filling on 04/12/2012.*
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-2, 4-10, 12-14, 25, and 28-33 .*
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *6/8/2012 .*
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Jing Sims/
Examiner, Art Unit 2437

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Aaron Emigh.* (3)____.

(2) *Jing Sims.* (4)____.

Date of Interview: *08 June 2012.*

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: ____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1, 6, 9, 14, and 24.*

Identification of prior art discussed: *Liang (US 7287278 B2).*

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☒ Attachment

/Jing Sims/ Examiner, Art Unit 2437	

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments:

Examiner and Inventor agreed to incorporated limitations in claim 24 to claim 1 (with similar amendments to claims 9 and 14) would place the claims in condition for allowance. Examiner and Inventor also agreed the minor modification in claim 6, and the cancellation for claim. The detailed amendment has shown as below:

1. (currently amended) A method for protecting a network, comprising:
detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and
permitting the first host to communicate with [[a]] the remediation host.

6. (currently amended) A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes:
detecting an outbound communication from the first host; and
forwarding the outbound communication if it is addressed to [[a]] the remediation host.

9. (currently amended) A system for protecting a network, comprising:
a processor configured to:
detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and
permit the first host to communicate with [[a]] the remediation host; and
a memory coupled to the processor and configured to provide instructions to the processor.

14. (currently amended) A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:
detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

DETAILED ACTION

This Examiner Amendment and Reasons for Allowance action is in response to the filing on 04/12/2012.

EXAMINER'S AMENDMENT

1. 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 Inventor Aaron Emigh on 06/08/2012.

2. Replacing Claims 1, 6, 9, 14, and 24 as following:

Claim 1: (currently amended) A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has

ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~.

Claim 6: (currently amended) A method as recited in claim 1, wherein ~~preventing the first host from sending data to the one or more other hosts~~ permitting the first host to communicate with the remediation host includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to [[a]] the remediation host.

Claim 9: (currently amended) A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification

page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permit the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition.~~; and

a memory coupled to the processor and configured to provide instructions to the processor.

Claim 14: (currently amended) A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by

preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~.

Claim 24: (canceled)

Allowance

3. Claims 1-2, 4-10, 12-14, 25, and 28-33 are allowed.

4. Claims 1, 6, 9, 14 have been amended which overcome the Examiner's prior rejections, see paper of 10/12/2011. Examiner withdraws all outstanding rejections to claims 1-8, 9-14, and 25-33.

Examiner's Statement of Reasons for Allowance

5. The following is an examiner's statement of reasons for allowance:

The present invention is directed to a method, a system, and a computer program product detecting an insecure condition on a host computer on a protected network. it verifies cleanliness of the host computer by contacting a trusted platform module within the host computer, and once detected the host computer is insecure, it limits the host computer is quarantined to prevent contagion. The host computer is limited only be able to can communicate with a quarantine server not any other host until it has been remedied.

Independent claim 1, 9, and 14 recite the uniquely distinct features of “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host; when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page

to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and permitting the first host to communicate with the remediation host".

The closest prior art, Liang (US 7287278 B2) and Yan et al. (US 2005/0033987 A1 disclose detecting abnormal events on host, and redirecting to quarantine serve to get remediated; however, they fail to anticipate or render serving both the specific quarantine notification page with the DNS redirection when in combination with the remaining claim limitations.

Therefore the claims are allowable over the cited prior art.

Dependent claims are allowed as they depend from allowable independent claims.

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 Reason for Allowance".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 9:00am-5:00pm EST, Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on (571)272-3867. 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.

/Jing Sims/
Examiner, Art Unit 2437

/Eleni A Shiferaw/

Supervisory Patent Examiner, Art Unit 2437

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
11237003	ROSKIND ET AL.
Examiner	**Art Unit**
JING SIMS	2437

ORIGINAL	
CLASS	SUBCLASS
726	22

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	23	24	25		

INTERNATIONAL CLASSIFICATION

CLAIMED	NON-CLAIMED
G 0 6 F 11 / 00 (2006.01.01)	
G 0 6 F 12 / 14 (2006.01.01)	
G 0 6 F 12 / 16 (2006.01.01)	
G 0 8 B 23 / 00 (2006.01.01)	

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17	18	33										
2	2		18												
	3		19												
3	4		20												
4	5		21												
5	6		22												
6	7		23												
7	8		24												
12	9	8	25												
13	10		26												
	11		27												
14	12	9	28												
15	13	10	29												
19	14	11	30												
	15	16	31												
	16	17	32												

/JING SIMS/ Examiner.Art Unit 2437	06/08/2012	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	19	
/ELENI SHIFERAW/ Supervisory Patent Examiner.Art Unit 2437	06/12/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	10B

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	Art Unit
	JING SIMS	4148

SEARCHED

Class	Subclass	Date	Examiner
726	22,23	11/3/2008	JS
726	11,14, 22-25	6/8/2012	JS

SEARCH NOTES

Search Notes	Date	Examiner
Inventor search in EAST	11/7/2008	JS
Text Search (see EAST notes)	11/7/2008	JS
Updated EAST Search	06/29/2009	JS
Google Patent Search	06/29/2009	JS
Google Scholar Search	06/29/2009	JS
IEEE Search	06/29/2009	JS
Updated EAST search	07/15/2010	JS
Google scholar search	07/15/2010	JS
Plus search	07/15/2010	JS
Updated EAST full text search	10/4/2011	JS
Consulted the re-open non-final OA with Primary Examiner	10/4/2011	JS
Updated EAST full text search	6/8/2012	JS
Updated IEEE search	6/8/2012	JS
Updated ACM search	6/8/2012	JS
Reviewd, searched, and consulted by Primary Examiner	6/8/2012	JS

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	11, 14, 22-25 combined with keywords search	6/8/2012	JS

/Jing Sims/
Examiner.Art Unit 2437

Sims, Jing

From: Sims, Jing
Sent: Tuesday, June 12, 2012 10:59 AM
To: 'Aaron Emigh'
Subject: RE: Amendment to Application No. 11/237,003

Dear Aaron Emigh,

The amendment showed in your latest Email is incorrect. The amendment has made on 04/12/2012 is not reflected in the amendment. Please be notice the highlighted paragraphs has been left out from the final version of the amendment. I believe you were working on older version of claim set.

The amendment shown in this email will be the final allowable version. If you have any questions, please don't hesitate to call or email.

Thank you,
Jing Sims

EXAMINER'S AMENDMENT

1. 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 Inventor Aaron Emigh on 06/08/2012.

2. Replacing Claims 1, 6, 9, 14, and 24 as following:

Claim 1: (currently amended) A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

Ex.1002
NETSKOPE, INC. / Page 55 of 378

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~.

Claim 6: (currently amended) A method as recited in claim 1, wherein ~~preventing the first host from sending data to the one or more other hosts~~ permitting the first host to communicate with the remediation host includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to [[a]] the remediation host.

Claim 9: (currently amended) A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or

Ex.1002
NETSKOPE, INC. / Page 56 of 378

more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permit the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~; and

a memory coupled to the processor and configured to provide instructions to the processor.

Claim 14: (currently amended) A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine

Ex.1002
NETSKOPE, INC. / Page 57 of 378

notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~.

Claim 24: (canceled)

From: Aaron Emigh [mailto:aaron@emigh.org]
Sent: Friday, June 08, 2012 11:24 PM
To: Sims, Jing
Subject: RE: Amendment to Application No. 11/237,003

Addendum: I would also like to confirm the cancellation of claim 24.

Yours,
Aaron Emigh

From: Aaron Emigh [mailto:aaron@emigh.org]
Sent: Friday, June 08, 2012 8:18 PM
To: 'Sims, Jing'
Subject: Amendment to Application No. 11/237,003

Examiner Sims –

Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail. I understand that a copy of these communications will be made of record in the application file.

Aaron Emigh

/Aaron T. Emigh/ (electronic signature)

I would like to confirm the following amendments to claims 1, 6, 9, and 14:

1. (currently amended) A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server

Ex.1002
NETSKOPE, INC. / Page 58 of 378

request, and in the event the service request comprises a DNS query, providing in response an IP address of a guarantine server configured to serve the guarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~.

6. (currently amended) A method as recited in claim 1, wherein ~~preventing the first host from sending data to the one or more other hosts~~ permitting the first host to communicate with the remediation host includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to [[a]] the remediation host.

9. (currently amended) A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a guarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a guarantine server configured to serve the guarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permit the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~; and

a memory coupled to the processor and configured to provide instructions to the processor.

14. (currently amended) A computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing

Ex.1002
NETSKOPE, INC. / Page 59 of 378

base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with [[a]] the remediation host ~~configured to provide data usable to remedy the insecure condition~~.

Thank you for your time and attention to this matter.

Yours,
Aaron Emigh

Ex.1002
NETSKOPE, INC. / Page 60 of 378

IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites

Cart(0) | Create Account | Sign In

IEEE Xplore DIGITAL LIBRARY

Access provided by:
United States Patent and Trademark Office
Sign Out

IEEE

BROWSE | MY SETTINGS | WHAT CAN I ACCESS? | SUBSCRIBE | HELP | CONTACT US

SEARCH

Advanced Search | Preferences | Search Tips | More Search Options

REFINE SEARCH

Search within results:

Search

Only show full text results included in my subscription

CONTENT TYPE

Conference Publications (3)
Journals & Magazines (2)

PUBLICATION YEAR

Single Year Range

2003 2012

From: 2003

To: 2012

AUTHOR

Singh, V. (1)
Shah, H. (1)
Shyamasundar, R.K. (1)
Hui Chen (1)
Ozdemir, S. (1)
Jing Liu (1)
Ray, C. (1)
Yang Xiao (1)
Charney, S. (1)
Dodle, S. (1)
Yang Xinfeng (1)
Kumar, N.V.N. (1)
Yao Yuxian (1)
Li Lianhuan (1)

AFFILIATION

PUBLICATION TITLE

TOPIC

CONFERENCE LOCATION

1. **Collective Defense: Applying the Public-Health Model to the Internet**

   Charney, S.
   Security & Privacy, IEEE
   Volume: 10 , Issue: 2
   Digital Object Identifier: 10.1109/MSP.2011.152
   Publication Year: 2012 , Page(s): 54 - 59
   IEEE JOURNALS & MAGAZINES

   Quick Abstract | PDF (1757 KB)

2. **Can we certify systems for freedom from malware**

   Kumar, N.V.N.; Shah, H. ; Shyamasundar, R.K.
   Software Engineering, 2010 ACM/IEEE 32nd International Conference on
   Volume: 2
   Digital Object Identifier: 10.1145/1810295.1810323
   Publication Year: 2010 , Page(s): 175 - 178
   IEEE CONFERENCE PUBLICATIONS

   Quick Abstract | PDF (108 KB)

3. **Analysis and comparison on new network security access technology-NAC and NAP**

   Yao Yuxian; Li Lianhuan; Yang Xinfeng
   Computer Science and Network Technology (ICCSNT), 2011 International Conference on
   Volume: 3
   Digital Object Identifier: 10.1109/ICCSNT.2011.6182336
   Publication Year: 2011 , Page(s): 1877 - 1880
   IEEE CONFERENCE PUBLICATIONS

   Quick Abstract | PDF (750 KB)

4. **A modest proposal: licensing personal computers and Internet service providers**

   Ray, C.
   Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society
   Digital Object Identifier: 10.1109/SMCSIA.2003.1232414
   Publication Year: 2003 , Page(s): 151 - 157
   IEEE CONFERENCE PUBLICATIONS

SEARCH HISTORY BETA

NEW! Search History BETA is now available using your personal IEEE account.

DICTIONARY

Browse Standards Dictionary

» Quick Abstract | PDF (656 KB)

☐ **A Survey of Payment Card Industry Data Security Standard**

Jing Liu; Yang Xiao; Hui Chen; Ozdemir, S.; Dodle, S.; Singh, V.

Communications Surveys & Tutorials, IEEE

Volume: 12 , Issue: 3

Digital Object Identifier: 10.1109/SURV.2010.031810.00089

Publication Year: 2010 , Page(s): 287 - 303

Cited by 2

IEEE JOURNALS & MAGAZINES

» Quick Abstract | PDF (1094 KB)

Sort by: Relevance

Select All on Page | Deselect All

Sign In | Create Account

IEEE Account
» Change Username/Password
» Update Address

Purchase Details
» Payment Options
» Order History
» Access Purchased Documents

Profile Information
» Communications Preferences
» Profession and Education
» Technical Interests

Need Help?
» US & Canada: +1 800 678 4333
» Worldwide: +1 732 981 0060
» Contact & Support

About IEEE Xplore | Contact | Help | Terms of Use | Nondiscrimination Policy | Site Map | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest professional association for the advancement of technology.

© Copyright 2012 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	51	(detect$3 determin$3 observ$3 identify$3 perceiv$3 monitor$3) with (insecure virus worm attack trojan) same (isolat$3 quarantine remed$5 remedat$3) and ((redirect$3 rerout$3 rout$3) near5 (webpage page))	US-PGPUB; USPAT; FPRS; EPO; JPO; IBM_TDB	OR	ON	2012/06/08 23:02
L5	51	(detect$3 determin$3 observ$3 identify$3 perceiv$3 monitor$3) with (insecure virus worm attack trojan) same (isolat$3 quarantine remed$5) and ((redirect$3 rerout$3 rout$3) near5 (webpage page))	US-PGPUB; USPAT; FPRS; EPO; JPO; IBM_TDB	OR	ON	2012/06/08 23:03
L6	80	(detect$3 determin$3 observ$3 identify$3 perceiv$3 monitor$3) with (insecure virus worm attack trojan) same (isolat$3 quarantine remed$5) and ((redirect$3 rerout$3 rout$3) near5 (webpage link hyperlink weblink))	US-PGPUB; USPAT; FPRS; EPO; JPO; IBM_TDB	OR	ON	2012/06/08 23:03
L7	2	(detect$3 determin$3 observ$3 identify$3 perceiv$3 monitor$3) with (insecure virus worm attack trojan) same (isolat$3 quarantine remed$5) and ((redirect$3 rerout$3 rout$3) near5 (webpage link hyperlink weblink) with DNS)	US-PGPUB; USPAT; FPRS; EPO; JPO; IBM_TDB	OR	ON	2012/06/08 23:03
L8	26	(detect$3 determin$3 observ$3 identify$3 perceiv$3 monitor$3) with (insecure virus worm attack trojan) same (isolat$3 quarantine remed$5) and ((redirect$3 rerout$3 rout$3) near5 (webpage link hyperlink weblink)) and 726/11,14,22-25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; IBM_TDB	OR	ON	2012/06/08 23:29
L12	8779	726/11,14,22-25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; IBM_TDB	OR	ON	2012/06/08 23:40

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	0	(detect$3 near5 insecure near3 host with (protected adj2 network) same (trusted near2 computing near2 base) same (attestation near2 cleanliness) same (quarantin)).clm.	US-PGPUB; USPAT	OR	ON	2012/06/08 23:33
L10	0	(detect$3 near5 insecure with network same (trusted near2 computing near2 base) same (attestation near2 cleanliness) same (quarantin)).clm.	US-PGPUB; USPAT	OR	ON	2012/06/08 23:33
L11	0	(quarantine near2 notification near2 page with (remediation) same redirect$3).clm.	US-PGPUB;	OR	ON	2012/06/08 23:35

			USPAT			
L13	4310	726/11,14,22-25.ccls.	USPAT	OR	ON	2012/06/08 23:40

6/9/2012 12:01:07 AM
C:\Users\jsims2\Documents\EAST\Workspaces\11237003.wsp

US Patent & Trademark Office

SIGN IN SIGN UP

Searching for: (quarantine and remedy) and (insecure or virus or trojan or worm or attack or malware) (start a new search)

Found **7** within *The ACM Guide to Computing Literature* (Bibliographic citations from major publishers in computing)

Limit your search to Publications from ACM and Affiliated Organizations (Full-Text collection: **344,935** items)

REFINE YOUR SEARCH

Refine by Keywords

Refine by People
Names
Institutions
Authors

Refine by Publications
Publication Year
Publication Names
ACM Publications
All Publications
Content Formats
Publishers

Refine by Conferences
Sponsors
Events
Proceeding Series

ADVANCED SEARCH
Advanced Search

FEEDBACK
Please provide us with feedback

Found **7** of **1,901,025**

Search Results Related SIGs

Results 1 - 7 of 7 Sort by relevance in expanded form

1 News: Zotob and VoIP
Joe O'Halloran
September 2005 **Network Security** , Volume 2005 Issue 9
Publisher: Elsevier Science Publishers B. V.

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 0

Voice over IP networks are with us, with more and more force. Future malware may well have a field day.

2 Expanding help desk services: the benefits of student S.O.S.
Lea H. Snyder
September 2003 **SIGUCCS '03:** Proceedings of the 31st annual ACM SIGUCCS fall conference
Publisher: ACM Request Permissions
Full text available: Pdf (295.64 KB)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 19, Downloads (Overall): 393, Citation Count: 0

It is a given fact that information technology managers often must make decisions on how to best serve the community at large while most effectively utilizing the manpower and resources available to them. Many Help Desks have expanded services by offering ... **Keywords**: accountability, customer service, help desk, management, measurement, on-site assistance, performance, student consultants, student staff

3 ResNet management: Wayne State University's experience supporting cisco clean access agent
Stephen Wassef, Rodrigo Reis, Dragan Lazin
November 2005 **SIGUCCS '05:** Proceedings of the 33rd annual ACM SIGUCCS fall conference
Publisher: ACM Request Permissions
Full text available: Pdf (224.33 KB)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 19, Downloads (Overall): 1203, Citation Count: 0

Wayne State University (WSU) has implemented network registration and management tools. These tools have matured and become very useful to reduce support costs and maintain continuity of network services for our residential network (ResNet) customers. ... **Keywords**: LDAP ID used for network authentication, M*A*S*H - a great TV series used to name our PC clinics (MASH), WSU accessID, cisco clean access agent (CCAA), digital millennium copyright act (DMCA), dynamic host configuration protocol (DHCP), lightweight directory access protocol (LDAP), motion picture association of America (MPAA), recording industry association of America (RIAA)

4 Infrastructures for information technology systems: perspectives on their evolution and impact

Ex.1002
NETSKOPE, INC. / Page 65 of 378

C. V. Ramamoorthy, Remzi Seker

May 2004 **SERA'04:** Proceedings of the Second international conference on Software Engineering Research, Management and Applications

Publisher: Springer-Verlag

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 0

This paper attempts to clarify infrastructure's definition and its impact and reach. Despite the wide use of the term and the importance of the entities it represents, the notion of infrastructures has not been thoroughly addressed. We use different ...

5 Wireless security patch management system

Charles Higby, Michael Bailey

October 2004 **CITC5 '04:** Proceedings of the 5th conference on Information technology education

Publisher: ACM Request Permissions

Full text available: Pdf (526.37 KB)

Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 38, Downloads (Overall): 1206, Citation Count: 0

Wireless access on college campuses facilitates the spread of computer viruses and worms due to laptops that do not have current software patches and/or antivirus protection connecting to the network. Wireless local area networks provide a luxury of ...

Keywords: administration, configuration, patch, security, update, virus, wireless, worm

6 Events: Events calendar

September 2005 **Network Security** , Volume 2005 Issue 9

Publisher: Elsevier Science Publishers B. V.

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 0

7 Simple Semantics in Topic Detection and Tracking

Juha Makkonen, Helena Ahonen-Myka, Marko Salmenkivi

September 2004 **Information Retrieval** , Volume 7 Issue 3-4

Publisher: Kluwer Academic Publishers

Full text available: Publisher Site

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 23

Topic Detection and Tracking (TDT) is a research initiative that aims at techniques to organize news documents in terms of news events. We propose a method that incorporates simple semantics into TDT by splitting the term space into groups of terms that ...

Keywords: geographical ontology, information extraction, retrieval model, temporal expression, topic detection and tracking

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2012 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	2437

✓	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	11/07/2008	06/29/2009	04/22/2010	07/15/2010	10/05/2011	06/08/2012			
	1	✓	✓	÷	✓	✓	=			
	2	✓	✓	÷	✓	✓	=			
	3	✓	-	-	-	-	-			
	4	✓	✓	÷	✓	✓	=			
	5	✓	✓	÷	✓	✓	=			
	6	✓	✓	÷	✓	✓	=			
	7	✓	✓	÷	✓	✓	=			
	8	✓	✓	÷	✓	✓	=			
	9	✓	✓	÷	✓	✓	=			
	10	✓	✓	÷	✓	✓	=			
	11	✓	-	-	-	-	-			
	12	✓	✓	÷	✓	✓	=			
	13	✓	✓	÷	✓	✓	=			
	14	✓	✓	÷	✓	✓	=			
	15	✓	✓	÷	÷	÷	-			
	16	✓	✓	÷	÷	÷	-			
	17	✓	✓	÷	÷	÷	-			
	18	✓	✓	÷	÷	÷	-			
	19	✓	-	-	-	-	-			
	20	✓	-	-	-	-	-			
	21		✓	÷	÷	÷	-			
	22		✓	÷	÷	÷	-			
	23		✓	÷	÷	÷	-			
	24		✓	÷	✓	✓	-			
	25		✓	÷	✓	✓	=			
	26		✓	-	-	-	-			
	27		✓	-	-	-	-			
	28						=			
	29						=			
	30						=			
	31						=			
	32						=			
	33						=			

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: April 12, 2012.

/Aaron T. Emigh/
Aaron Emigh

AMENDMENT C

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

Dear Sir:

This is in response to the Office Action mailed October 12, 2011. The following amendments and remarks are respectfully submitted.

IN THE CLAIMS

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

Listing of Claims:

1. (currently amended) A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

2. (currently amended) A method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data, ~~checking a configuration or setting, determining whether a security data is up to date,~~ determining whether a security software is installed, and detecting anomalous network traffic~~, and determining that an available patch has not been installed~~.

3. (canceled)

4. (original) A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.

5. (original) A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

6. (original) A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to a remediation host.

7. (original) A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.

8. (original) A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

9. (currently amended) A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and

a memory coupled to the processor and configured to provide instructions to the processor.

10. (currently amended) A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, ~~checking a configuration or setting, determining whether a security data is up to date,~~ determining whether a security software is installed, and detecting anomalous network traffic~~, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion~~.

11. (canceled)

12. (previously presented) A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.

13. (original) A system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

14. (currently amended) A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable ~~storage~~ medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

15-23. (canceled)

24. (previously presented) A method as recited in claim 1, further comprising:

receiving a service request sent by the first host;

serving a quarantine notification page to the first host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

25. (previously presented) A method as recited in claim 1, performed at an Internet service provider.

26. (canceled)

27. (canceled)

28. (new) A method as recited in claim 1, wherein the software component on the first host is an operating system.

29. (new) A method as recited in claim 1, wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.

30. (new) A method as recited in claim 1, wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.

31. (new) A system as recited in claim 9, wherein the software component on the first host is an operating system.

32. (new) A system as recited in claim 9, wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.

33. (new) A system as recited in claim 32, wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.

REMARKS

Claims 1, 2, 4-10, 12-14, 24-25, and 28-33 are pending. Claims 1, 2, 9, 10, and 14 have been amended. New claims 28-33 have been added. Support for the amendments and new claims can be found without limitation at paragraph 50, and Figure 13, of the specification.

The Examiner has rejected claim 14 under 35 USC 101 on the basis that a "computer readable storage medium" could be a signal, and has suggested reciting a "non-transitory" medium instead. Claim 14 has been amended according to the Examiner's suggestion and is believed to be allowable.

The Examiner has rejected claims 1, 2, 4-10, and 12-14 under 35 USC 103(a) as being unpatentable over Liang (US 7,287,278) in view of Yan et al (US 2005/0033987), hereinafter referred to as Yan.

Neither Liang nor Yan, alone or in combination, appear to teach or suggest "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host," as recited in amended independent claims 1, 9, and 14.

Claims 1, 9, and 14 are therefore believed to be allowable.

Claims 2 and 4-8 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claims 10, 12, and 13 depend from claim 9 and are believed to be allowable for the same reasons described above.

The Examiner has rejected claim 24 under 35 USC 103(a) as being unpatentable over Liang in view of Yan, further in view of Lewis et al (US Pub. No. 2005/0131997 A1), hereinafter referred to as Lewis.

Neither Liang, Yan, nor Lewis, alone or in combination, appear to teach or suggest "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host," as recited in amended claim 1.

Claim 24 depends from claim 1 and is believed to be allowable for the same reasons described above.

The Examiner has rejected claim 25 under 35 USC 103(a) as being unpatentable over Liang in view of McElhaney, Jr., et al (US Patent No. 6,823,479 B1), hereinafter referred to as McElhaney.

Neither Liang nor McElhaney, alone or in combination, appear to teach or suggest "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host," as recited in amended independent claim 1.

Claim 25 depends from claim 1 and is believed to be allowable for the same reasons described above.

New claims 28-30 depend from claim 1 and are believed to be allowable for the same reasons described above.

New claims 31-33 depend from claim 9 and are believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: April 12, 2012

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237003
Filing Date:	27-Sep-2005
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-034

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	2253	1	635	635

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**635**

Electronic Acknowledgement Receipt

EFS ID:	12522910
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	12-APR-2012
Filing Date:	27-SEP-2005
Time Stamp:	03:53:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$635
RAM confirmation Number	11969
Deposit Account	504831
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		PB-034-amendment-c.pdf	86924 7e2af909cb0959dfa4da6395500773f26b415f62	yes	8

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	8

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	29724 c2c61d286df6af71966795dbcd567403e057ba1f	no	2

Warnings:

Information:

Total Files Size (in bytes):	116648

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/237,003	Filing Date 09/27/2005	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	x $ =		OR	x $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	x $ =			x $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**04/12/2012**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 23	=	x $ =		OR	x $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***5	=	x $ =		OR	x $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/ELMIRA HALL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 10/12/2011

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/12/2011	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.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2011*.

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

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,2,4-10,12-14,24 and 25* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,2,4-10,12-14,24 and 25* is/are rejected.

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

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

Application Papers

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

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on July 19, 2011, PROSECUTION IS HEREBY REOPENED. New Grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Rejections - 35 USC § 101

2. 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.

3. Claim 14 is directed to non-statutory subject matter. The decision on whether this claim is statutory or not would depend on whether or not the specification defines “a computer readable storage medium” as not being a signal otherwise the ordinary

meaning in the art that "a computer readable storage medium" can be a signal is rule and the claim is not statutory.

The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media (or non-transitory media) and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media, particularly when the specification is **silent** (or absent of a controlling definition in the specification)**.** See MPEP §2111.01. When the broadest reasonable interpretation of a claim covers a signal per se, the claim must be rejected under 35 U.S.C. § 101 as covering non-statutory subject matter. See In re Nuijten, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter); see Interim Examination Instructions for Evaluating Subject Matter Eligibility under 35 U.S.C. § 101, Aug. 24, 2009; p. 2 and Official Gazette Notice link:

http://www.uspto.gov/web/offices/com/sol/og/2010/week08/TOC.htm#ref20 or Subject Matter Eligibility of Computer Readable Media (26Jan2010) 1351 OG 21223FEB2010

Non acceptable

variations may be "machine (or computer) readable (or accessible or usable) storage medium", "recording medium", "tangible (or physical) machine (or computer) readable (or accessible or usable) storage medium"

Note: a "tangible medium" includes transitory propagating signals as the modifier/adjective "tangible" means capable of being touched or perceived and signal (e.g. sound) can be perceived.

Possible fix:

Amend the claimed term to: "non-transitory", "computer usable memory", or "computer usable storage memory", "computer readable memory", "computer readable device", (i.e. any variations thereof, where **"media" or "medium"** is replaced by "**device**" or "**memory**") or adding "wherein the medium is not a signal".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 2, 4-10, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liang (US 7287278 B2) in view of Yan et al. (US 2005/0033987 A1, hereinafter, Yan)**.

As per claim 1, Liang discloses "a method for protecting a network, comprising":

"detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present), "quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a

virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

Liang discloses detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device; however, Liang does not discloses detecting the insecure condition includes contacting a trusted computing based associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness.

Yan discloses **detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module** (e.g., [0019], [0055], [0077]: seeking to know the state of the computing environment inside TPS 100 depends on the value of the integrity metrics; wherein a trusted computing base corresponding with a mechanism that provide the security related integrity metrics checking to the computing system), and **the response includes a valid digitally signed attestation of cleanliness** (e.g., [0055], [0077]: TPM 130 proclaims its trustworthiness by signing data using one of its identities, the signature key is known only to TPM 130 and is the private key of a key pair).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device as described by Liang and add the insecure condition includes contacting a trusted computing base associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness as taught by Yan because it would

improve trust in one platform with eventual trust provide by the trusted computing platform and promotes the concept of a trusted subsystem and chains of trust between such subsystems (see Yan, [0003]).

As per claim 2, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 4, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed" (col. 8 line 55-64, if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 5, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system" (col. 17, line 47-55, identifying a new client device to e added to the network. Identification includes identifying the type of system, resident operating system etc. In col. 18, line 4-7, if the new client has been determined that proper anti-virus policies and protocols are not in place, then all access to all addresses except to that of an anti-virus software installation server are blocked. Liang teaches the client need to meet certain safety policies and protocols to access the network. The initial startup after installation of the operating system is the configuration of the system; therefore, it is the policies and protocols).

As per claim 6, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular those data packets found to be virus-free are sent back to the network traffic flow).

As per claim 7, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular data packets deemed more likely to be affected are passed directly to the file scan module. A data packet is always has its purpose to request service from the destination network and it is usually not address to a remediation host).

As per claim 8, Liang discloses "a method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 9, Liang discloses "a system for protecting a network, comprising: a processor configured to":

"detect an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor monitors activities of network, detecting abnormal events from other computers that on the network. Liang also describes virus monitors can be a stand alone server computer in col. 7, line 15-21), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"and permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak) "and a memory coupled to the processor and configured to provide instructions to the processor" (col. 7, line 15-21, virus monitors can be a stand alone server computer. Every stand alone computer includes memory and processor).

Liang discloses detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device; however, Liang does not discloses detecting the insecure condition includes contacting a trusted computing based associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness.

Yan discloses **detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module** (e.g., [0019], [0055], [0077]: seeking to know the state of the computing environment inside TPS 100 depends on the value of the integrity metrics; wherein a trusted computing base corresponding with a mechanism that provide the security related integrity metrics checking to the computing system), and **the response includes a valid digitally signed attestation of cleanliness** (e.g., [0055], [0077]: TPM 130 proclaims its trustworthiness by signing data using one of its identities, the signature key is known only to TPM 130 and is the private key of a key pair).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify detecting an insecure condition in a client computing

device and receiving an response of the cleanliness of the client computing device as described by Liang and add the insecure condition includes contacting a trusted computing base associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness as taught by Yan because it would improve trust in one platform with eventual trust provide by the trusted computing platform and promotes the concept of a trusted subsystem and chains of trust between such subsystems (see Yan, [0003]).

As per claim 10, Liang discloses "a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 12, Liang discloses "a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed" (col. 7, line 25-36, the controller includes a rules engine used to store and source of detection rules for detecting computer viruses and an outbreak prevention policy distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak. Liang also discloses the policies, protocols and procedures can be periodically updated. Checking initial startup after installation of an OS is regular procedure to perform for securing of a computer, therefore the rules, polices, or procedures that Liang described include that checking initial startup after installation of an OS).

As per claim 13, Liang discloses "a system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 14, Liang discloses “a computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for” (col. 3, line 44-45, and line 59-67, a computer program project for monitoring a network for computer viruses):

“detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host” (col. 8, lines 49-53, send a query to client device requesting confirmation);

“and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)”;

“when it is determined that the response does not include a valid digitally signed attestation of cleanliness” (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems);

"and permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

Liang discloses detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device; however, Liang does not discloses detecting the insecure condition includes contacting a trusted computing based associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness.

Yan discloses **detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module** (e.g., [0019], [0055], [0077]: seeking to know the state of the computing environment inside TPS 100 depends on the value of the integrity metrics; wherein a trusted computing base corresponding with a mechanism that provide the security related integrity metrics checking to the computing system), and **the response includes a valid digitally**

signed attestation of cleanliness (e.g., [0055], [0077]: TPM 130 proclaims its trustworthiness by signing data using one of its identities, the signature key is known only to TPM 130 and is the private key of a key pair).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device as described by Liang and add the insecure condition includes contacting a trusted computing base associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness as taught by Yan because it would improve trust in one platform with eventual trust provide by the trusted computing platform and promotes the concept of a trusted subsystem and chains of trust between such subsystems (see Yan, [0003]).

5. **Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of Lewis**.

As per claim 24, claim 1 is incorporated and, Lewis discloses further comprising:

receiving a service request sent by the first host; serving a quarantine notification page to the first host if the service request comprises a web server request" (page 8, [0083], lines 20-22, wherein a quarantine notification page corresponding to fix-up page on QS, QS stands for quarantine server);

"and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host" (page 8, [0082], the purpose is to prevent the unsafe machine from talking to any other network node except for the few select severs it can use to update it compliance with network security policy; [0083], whenever the client performs name resolution on any address, it will receive the IP of quarantine server. This way any client will be redirected to fix-up page on quarantine server).

Liang and Lewis are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host as described by Liang and add the host request service including DNS and other requests as taught by Lewis because it would be added more detailed of the normal services that request from a host to a server in a secured network.

6. **Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of McElhaney, Jr. et al. (US patent no. US 6,823,479 B1) (hereinafter McElhaney)**.

As per claim 25, in claim 1 is incorporated, and McElhaney discloses "performed at an Internet service provider" (col. 1, line 26-35, ISP provides test tools to protect subscribers by isolate the damaged root).

Liang and McElhaney are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host in a distributed network as described by Liang and add the distributed network also can an ISP as taught by McElhaney because it would be logically expanded the network to an distributed network work such as an Internet Service Provider.

Examiner Notes

7. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jing Sims whose telephone number is (571)270-7315. The examiner can normally be reached on 9:00am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. 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.

/Jing Sims/
Examiner, Art Unit 2437
/Eleni A Shiferaw/

Supervisory Patent Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/237,003	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner JING SIMS	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0033987 A1	02-2005	Yan et al.	713/201
*	B	US-7,424,610 B2	09-2008	Ranganathan, Kumar	713/164
*	C	US-7,263,720 B2	08-2007	Silvester, Kelan C.	726/22
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	4148

✓	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	11/07/2008	06/29/2009	04/22/2010	07/15/2010	10/05/2011				
	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		✓	-	-	-				

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"11237003"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/05 08:48
S1	0	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) near6 (clean$6 free up$1to$1date trusted secured) near5 host and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:18
S2	29	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) near6 (clean$6 free up$1to$1date trusted secured) and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:18
S3	0	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) near6 (clean$6 free up$1to$1date secured) and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:19
S4	1	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) same (clean$6 free up$1to$1date secured) and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:19

S5	3	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) same (attestation confirmation proof verification) and 726/22-25.ccls. and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:23
S6	8	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) and 726/22-25. ccls. and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:27
S7	4	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) same (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) same integrity and 726/22-25.ccls. and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/04 11:38
S8	46	(((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) same (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))) same integrity and @ad<"20040927"	US-PGPUB; USPAT; USOCR	OR	ON	2011/10/0 11:38
S9	3	"20050033978"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	ON	2011/10/04 16:28
S10	3	"20050033987"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	ON	2011/10/04 16:29

S11	2	"20050033987" and ((((trusted adj platform adj module) ("TPM")) (trusted adj computing adj base)) near6 (sign$5 ((encrypt$3 scrambl$3 encipher$3 cipher$3) near3 (private adj key))))	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	ON	2011/10/04 16:30

10/5/2011 9:09:42 AM
C:\Documents and Settings\jsims2\My Documents\EAST\Workspaces\11237003_Appeal.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	Art Unit
	JING SIMS	4148

SEARCHED

Class	Subclass	Date	Examiner
726	22,23	11/3/2008	JS

SEARCH NOTES

Search Notes	Date	Examiner
Inventor search in EAST	11/7/2008	JS
Text Search (see EAST notes)	11/7/2008	JS
Updated EAST Search	06/29/2009	JS
Google Patent Search	06/29/2009	JS
Google Scholar Search	06/29/2009	JS
IEEE Search	06/29/2009	JS
Updated EAST search	07/15/2010	JS
Google scholar search	07/15/2010	JS
Plus search	07/15/2010	JS
Updated EAST full text search	10/4/2011	JS
Consulted the re-open non-final OA with Primary Examiner	10/4/2011	JS

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/Jing Sims/
Examiner.Art Unit 2437

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: July 19, 2011.

/Aaron T. Emigh/
Aaron Emigh

APPELLANT'S BRIEF PURSUANT TO 37 C.F.R. §41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appellant, Applicant in the above-captioned patent application and Manager of Radix Holdings, LLC, the assignee of record, appeals the final rejection of Claims 1, 2, 4-10, 12-14, 24, and 25 set forth in the final Office Action mailed on July 20, 2010.

I. REAL PARTY IN INTEREST

The real party of interest in the present application is Radix Holdings, LLC, the assignee of record.

II. RELATED APPEALS AND INTERFERENCES

PURSUANT TO 37 C.F.R. §41.37(c)(1)(ii), Appellant hereby notifies the Board of Patent Appeals that Appellant and the Assignee do not know of any appeals or interferences that will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 2, 4-10, 12-14, 24, and 25 are currently pending in the application, and are attached hereto as an appendix. Claims 3, 11, 15-23, 26, and 27 have been canceled. All pending claims were finally rejected by the Examiner and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

All Amendments as of Appellant's Amendment B, filed on January 10, 2010, are believed to have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Since the application is being prosecuted *pro se*, a summary of claimed subject matter is not required according to 37 CFR 41.37(c)(1).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2, 4-10, and 12-14 are anticipated under 35 USC 102(e) by Liang (US 7,872,278).

Whether claim 24 is unpatentable under 35 USC 103(a) over Liang in view of Lewis et al (US Pub. No. 2005/0131997), hereinafter referred to as Lewis.

Whether claim 25 is unpatentable under 35 U.S.C. 35 USC 103(a) over Liang in view of McElhaney, Jr., et al (US Patent No. 6,823,479 B1), hereinafter referred to as McElhaney.

VII. ARGUMENT

WHETHER CLAIMS 1, 2, 4-10, AND 12-14 ARE ANTICIPATED UNDER 35 USC 102(E) BY LIANG

For the reasons set forth below, Appellant respectfully submits that the Examiner has erred in maintaining the 35 U.S.C 102(e) rejection of Claims 1, 2, 4-10, and 12-14.

The MPEP, §2131, states that in order for a rejection under 35 USC 102 to be proper, "'The identical invention must be shown in as complete detail as is contained in the ... claim.' *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)." As will be shown below, Liang does not show the identical invention in complete detail, and therefore the Examiner erred in his rejection under 35 USC 102(e).

Claims 1, 9, and 14

Liang does not anticipate "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness," nor "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network," as recited in amended independent claims 1 and 14, and similarly in amended independent claim 9.

Liang does not teach "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host" because Liang does not teach either a trusted computing base or a trusted platform module.

The Examiner has cited Liang, column 8, lines 49-53 as anticipating "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host," as recited in claims 1, 9, and 14. However, the cited

passages of Liang read "For example, virus monitor 102-1 sends a query 140 *to each of the client devices* 110-116 requesting confirmation that each has installed therein the appropriate anti-virus software as determined by the policies contained in the OPP file 135…" (Liang, column 8, lines 49-53, emphasis added.) Nothing in this, or elsewhere in Liang, appears to teach or suggest "contacting a trusted computing base," nor "a trusted computing base associated with a trusted platform module within the first host," as recited in claims 1, 9, and 14.

"Trusted computing base" and "trusted platform module are terms of art with specific meanings that are in no way discussed in Liang. The Wikipedia entry for "Trusted Platform Module (http://en.wikipedia.org/wiki/Trusted_platform_module; retrieved January 10, 2010) begins, "In computing, Trusted Platform Module (TPM) is both the name of a published specification detailing a secure cryptoprocessor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device" (as designated in certain Dell BIOS settings[1]). The TPM specification is the work of the Trusted Computing Group. The current version of the TPM specification is 1.2 Revision 103, published on July 9, 2007." Reinforcing the industry adoption of this technology and standardization around the term of art used in the claims, this specification has also been adopted as ISO/IEC standard 11889. As for the term of art "trusted computing base," the final paragraph of the "Definition and characterization" section of the Wikipedia entry on "Trusted Computing Base" (http://en.wikipedia.org/wiki/Trusted_computing_base; retrieved January 10, 2010) states that "A given piece of hardware or software is a part of the TCB if and only if it has been designed to be a part of the mechanism that provides its security to the computer system."

Liang does not anticipate a trusted platform module, nor a trusted computing base associated with a trusted platform module. Indeed, Appellant discussed the previously presented amendment to claims 1, 9, and 14 with the Examiner and Supervisory Patent Examiner Emmanuel Moise on April 14, 2009. During that interview, the Examiner explicitly stated that she believed the language in these claims as amended in Amendment A and presented herein overcame Liang, as indeed, they appear to do.

However, in the Final Office Action, the Examiner acknowledged Appellant's argument that Liang does not teach these terms of art, but further argued that because Liang vaguely states that "any operating system" may be used, that this anticipates operating systems with trusted platform modules and a trusted computing base. This argument is erroneous on at least two counts. First, it is erroneous because a trusted platform is a hardware component and not merely an operating system component. Second, it is erroneous because *Liang does not actually teach these limitations*, nor does the Examiner argue that it does. As noted above, the *Suzuki* standard for a §102 rejection is that "the identical invention must be shown ***in as complete detail as is contained in the ... claim***." (Emphasis added.) Clearly, Liang does not disclose the detail in the claim, i.e. "a trusted computing base associated with a trusted platform module,"and therefore it cannot anticipate under 35 USC 102(e).

Liang does not teach "determining whether the response includes a valid digitally signed attestation of cleanliness."

The Examiner has cited Liang, column 8, lines 53-55 as anticipating "determining whether the response includes a valid digitally signed attestation of cleanliness." The cited section of Liang reads "Upon receiving the query 140, each of the client devices checks for confirmation that the appropriate anti-virus software is indeed present." This, as elsewhere in Liang, does not appear to teach or suggest a "valid digitally signed attestation of cleanliness."

Similarly, the Examiner has cited Liang, column 8, lines 55-59 as anticipating "when it is determined that the response does not include a valid digitally signed attestation of cleanliness." The cited section of Liang reads "If, say in the case of the client device 116, that [sic] it is determined that either no software is present or the installed software is not appropriate (based upon the policies of the OPP file 135, for example), the client device 116 is directed only to the anti-virus software installation server 138 and no other..." This, as elsewhere in Liang, does not appear to teach or suggest a "valid digitally signed attestation of cleanliness."

In response to Appellant's observation that Liang does not teach "a valid digitally signed attestation of cleanliness," the Examiner responded that "in a Linux equipped with trusted computing system [sic], the confirmation is in 'upon receiving the query 140, each of the client

device [sic] check for confirmation that the appropriate antivirus software is indeed present' (Liang: col. 8, lines 53-59) is [sic] corresponding to valid digitally signed attestation."

Again, the *Suzuki* standard for a §102 rejection is that "the identical invention must be shown ***in as complete detail as is contained in the ... claim***." (Emphasis added.) Clearly, since Liang does not disclose the detail in the claim, i.e. "a valid digitally signed attestation," and the Examiner is instead speculating as to what a "confirmation" might be that is *not* disclosed in Liang, it cannot anticipate under 35 USC 102(e).

The use of a trusted computing base, trusted platform module, and valid digitally signed attestation of cleanliness in detecting an insecure condition are significant innovations, as they can, for example, prevent false reports by ensuring that an attestation of cleanliness is reliable and the result of properly executed checks. Without the use of such techniques, approaches such as Liang are potentially vulnerable to false reports by infected machines, and may fail to quarantine such machines, resulting in higher infection rates and greater propagation of malicious software.

The Examiner has erred by improperly reading into Liang extremely innovative applications that are simply not taught by it. In doing so, the Examiner has improperly rejected claims 1, 9, and 14 under 35 USC 102(e).

Claims 2 and 4-8

Claims 2 and 4-8 depend from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claims 2 and 4-8. Therefore, the rejections of claims 2 and 4-8 are also erroneous.

Claims 10, 12, and 13

Claims 10, 12, and 13 depend from claim 9. As discussed above, the Examiner's rejection of claim 9 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claims 10, 12, and 13. Therefore, the rejections of claims 10, 12, and 13 are also erroneous.

WHETHER CLAIM 24 IS UNPATENTABLE UNDER 35 USC 103(A) OVER LIANG IN VIEW OF LEWIS

For the reasons set forth below, Appellant respectfully submits that the Examiner has erred in maintaining the 35 U.S.C 103(a) rejection of Claim 24.

Claim 24

Claim 24 depends from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claim 24. Therefore, the rejection of claim 24 is also erroneous.

WHETHER CLAIM 25 IS UNPATENTABLE UNDER 35 U.S.C. 35 USC 103(A) OVER LIANG IN VIEW OF MCELHANEY

For the reasons set forth below, Appellant respectfully submits that the Examiner has erred in maintaining the 35 U.S.C 103(a) rejection of Claim 25.

Claim 25

Claim 25 depends from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claim 25. Therefore, the rejection of claim 25 is also erroneous.

VIII. CLAIMS APPENDIX

1. A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

2. A method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed.

4. A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.

5. A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

6. A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to a remediation host.

7. A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.

8. A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

9. A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and

a memory coupled to the processor and configured to provide instructions to the processor.

10. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion.

12. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.

13. A system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

14. A computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

24. A method as recited in claim 1, further comprising:

receiving a service request sent by the first host;

serving a quarantine notification page to the first host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

25. A method as recited in claim 1, performed at an Internet service provider.

IX. EVIDENCE APPENDIX

Not Applicable.

X. RELATED PROCEEDINGS APPENDIX

Not Applicable.

Respectfully submitted,

Dated: July 19, 2011

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237003
Filing Date:	27-Sep-2005
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-034

Filed as Small 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:				
Filing a brief in support of an appeal	2402	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 4 months with $0 paid	2254	1	865	865
Miscellaneous:				
			Total in USD ($)	**1135**

Electronic Acknowledgement Receipt

EFS ID:	10555598
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	19-JUL-2011
Filing Date:	27-SEP-2005
Time Stamp:	21:03:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1135
RAM confirmation Number	6409
Deposit Account	504831
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	PB-034-appeal-brief.pdf	169736 36b3b4e0410f0a433b6a46c2875250a3d09749a5	no	13
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31609 802f67d0d825433cc98cb18dc54d84cbb1ec65da	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	201345		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: January 19, 2011.

/Aaron T. Emigh/
Aaron Emigh

NOTICE OF APPEAL

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

Sir:

Applicant(s) hereby appeal(s) to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The Commissioner is authorized to charge the small entity fee for this Notice of Appeal under 37 CFR §41.20(b)(1), and any other applicable fees, to Deposit Account No. 50-4831 (Applicant Docket No. PB-034).

Respectfully submitted,

Dated: January 19, 2011

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237003
Filing Date:	27-Sep-2005
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-034

Filed as Small 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:				
Notice of appeal	2401	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	555	555
Miscellaneous:				
			Total in USD ($)	**825**

Electronic Acknowledgement Receipt

EFS ID:	9257078
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	19-JAN-2011
Filing Date:	27-SEP-2005
Time Stamp:	01:25:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$825
RAM confirmation Number	7871
Deposit Account	504831
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of Appeal Filed	PB-034-appeal-notice.pdf	68654 7207694d1478e10806fd9e2cf50451a4c451cfa6	no	1
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	31525 b5058a878005c5f21c88e1c8698d0e976f5e7281	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	100179		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 07/20/2010

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
07/20/2010	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.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	Jing Sims	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2010.*

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

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-10,12-14,24 and 25* is/are pending in the application.

4a) Of the above claim(s) *3,11,26 and 27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-10,12-14,and 24-25* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application 11/237,003 filed on 09/27/2005; amendment filed on 01/10/2010.

2. In elected Group I, no claim is amended. No new claim has been added.

Response to Arguments

3. Applicant argued Liang does not appear to teach or suggest wherein detecting the insecure condition includes contacting a trusted computing based associated with the trusted platform module within the first hot on page 6 and 7 of the Remarks. Examiner respectfully disagrees. Liang discloses “the various monitors, controllers, and servers can be configured in any operating platform. For example, such platforms include embedded Linux, PC based Linux or Windows... Sun SPARC platform…" (col. 8, lines 20-25). Examiner considered originally, for example, the embedded Linux or PC based Linux system with a trusted computing system; therefore, the process of “virus monitor 102 actives of network 100 for abnormal events” (col. 9, lines 49-52) must involved with a trusted computing base associated with a trusted platform module. Linux system with TCB protection is known long before Liang’s reference (i.e. integrating a Trusted Computing Base Extension Server Session server into the Linux Operating system by Glover); Hence, Liang does teach or suggest a trusted platform or trusted computing base associated with a trusted platform module.

4. Applicant further argued Liang does not appear to teach or suggest a “valid digitally signed attestation of cleanliness” on page 7. Examiner respectfully disagrees

because in a Linux equipped with trusted computing system, the confirmation in “upon receiving the query 140, each of the client device check for confirmation that the appropriate antivirus software is indeed present" (Liang: col. 8, lines 53-59) is corresponding to valid digitally signed attestation.

Claim Rejections - 35 USC § 102

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

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

5. **Claims 1, 2, 4-10, and 12-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Liang (US 7287278 B2)**.

As per claim 1, Liang discloses “a method for protecting a network, comprising”:

“detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host” (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present), "quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

As per claim 2, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is

installed, detecting anomalous network traffic, and determining that an available patch has not been installed" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 4, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes 20 determining that the first host should be quarantined until an update to an operating system has been installed" (col. 8 line 55-64, if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 5, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system" (col. 17, line 47-55, identifying a new client device to e added to the network. Identification includes identifying the type of system, resident operating system etc. In col. 18, line 4-7, if the new client has been determined that proper anti-virus policies and protocols are not in

place, then all access to all addresses except to that of an anti-virus software installation server are blocked. Liang teaches the client need to meet certain safety policies and protocols to access the network. The initial startup after installation of the operating system is the configuration of the system; therefore, it is the policies and protocols).

As per claim 6, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular those data packets found to be virus-free are sent back to the network traffic flow).

As per claim 7, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular data packets deemed more likely to be affected are passed directly to the file scan module. A data packet is always has its purpose to request service from the destination network and it is usually not address to a remediation host).

As per claim 8, Liang discloses "a method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 9, Liang discloses "a system for protecting a network, comprising: a processor configured to":

"detect an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor monitors activities of network, detecting abnormal events from other computers that on the network. Liang also describes virus monitors can be a stand alone server computer in col. 7, line 15-21), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"and permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak) "and a memory coupled to the processor and configured to provide instructions to the processor" (col. 7, line 15-21, virus monitors can be a stand alone server computer. Every stand alone computer includes memory and processor).

As per claim 10, Liang discloses “a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data” (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) “checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion” (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 12, Liang discloses “a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed” (col. 7, line 25-36, the controller includes a rules engine used to store and source of detection rules for detecting computer viruses and an outbreak prevention policy distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak. Liang also discloses the policies, protocols and procedures can be periodically updated. Checking initial startup after installation of an OS is regular procedure to perform for securing of a computer, therefore the rules, polices, or procedures that Liang described include that checking initial startup after installation of an OS).

As per claim 13, Liang discloses “a system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition” (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 14, Liang discloses “a computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for” (col. 3, line 44-45, and line 59-67, a computer program project for monitoring a network for computer viruses):

“detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host” (col. 8, lines 49-53, send a query to client device requesting confirmation);

“and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)”;

“when it is determined that the response does not include a valid digitally signed attestation of cleanliness” (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems);

"and permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of Lewis**.

As per claim 24, Liang discloses claim 1, however, not the rest of the claim. Lewis discloses "a method as recited in claim 1, further comprising:

receiving a service request sent by the first host; serving a quarantine notification page to the first host if the service request comprises a web server request" (page 8, [0083], lines 20-22, wherein a quarantine notification page corresponding to fix-up page on QS, QS stands for quarantine server);

"and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host" (page 8, [0082], the purpose is to prevent the unsafe machine from talking to any other network node except for the few select severs it can use to update it compliance with network security policy; [0083], whenever the client performs name resolution on any address, it will receive the IP of quarantine server. This way any client will be redirected to fix-up page on quarantine server).

Liang and Lewis are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host as described by Liang and add the host request service including DNS and other requests as taught by Lewis because it would be added more detailed of the normal services that request from a host to a server in a secured network.

7. **Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of McElhaney, Jr. et al. (US patent no. US 6,823,479 B1) (hereinafter McElhaney)**.

As per claim 25, Liang discloses a method as recited in claim 1, however, not "performed at an Internet service provider".

McElhaney discloses "performed at an Internet service provider" (col. 1, line 26-35, ISP provides test tools to protect subscribers by isolate the damaged root).

Liang and McElhaney are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host in a distributed network as described by Liang and add the distributed network also can an ISP as taught by McElhaney because it would be logically expanded the network to an distributed network work such as an Internet Service Provider.

Examiner Notes

8. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jing Sims whose telephone number is (571)270-7315. The examiner can normally be reached on 9:00am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. 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.

/Jing Sims/

Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/237,003	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner Jing Sims	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0188173 A1	10-2003	Zimmer et al.	713/189
*	B	US-2002/0083328 A1	06-2002	Riordan, James	713/183
*	C	US-2006/0053426 A1	03-2006	Dive-Reclus et al.	719/328
	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	Mark V. Glover, Integrating a Trusted Computing Base Extension Server and Secure Session Server into the LINUX Operating System, September 2001, Naval Postgraduate School.
*	V	Pearson et al., Trusted Computing Platform: TCPA Technology in Context, 2003, Hewlett-Packard Books: Patricia Pekary.
	W	OLS: Linux and trusted computing, July 22 2005, http://lwn.net/Articles/144681/ (as lined on 07/15/2010).
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	4148

SEARCHED

Class	Subclass	Date	Examiner
726	22,23	11/3/2008	JS

SEARCH NOTES

Search Notes	Date	Examiner
Inventor search in EAST	11/7/2008	JS
Text Search (see EAST notes)	11/7/2008	JS
Updated EAST Search	06/29/2009	JS
Google Patent Search	06/29/2009	JS
Google Scholar Search	06/29/2009	JS
IEEE Search	06/29/2009	JS
Updated EAST search	07/15/2010	JS
Google scholar search	07/15/2010	JS
Plus search	07/15/2010	JS

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/Jing Sims/
Examiner.Art Unit 2437

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	4148

✓	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	11/07/2008	06/29/2009	04/22/2010	07/15/2010					
	1	✓	✓	÷	✓					
	2	✓	✓	÷	✓					
	3	✓	-	-	-					
	4	✓	✓	÷	✓					
	5	✓	✓	÷	✓					
	6	✓	✓	÷	✓					
	7	✓	✓	÷	✓					
	8	✓	✓	÷	✓					
	9	✓	✓	÷	✓					
	10	✓	✓	÷	✓					
	11	✓	-	-	-					
	12	✓	✓	÷	✓					
	13	✓	✓	÷	✓					
	14	✓	✓	÷	✓					
	15	✓	✓	÷	÷					
	16	✓	✓	÷	÷					
	17	✓	✓	÷	÷					
	18	✓	✓	÷	÷					
	19	✓	-	-	-					
	20	✓	-	-	-					
	21		✓	÷	÷					
	22		✓	÷	÷					
	23		✓	÷	÷					
	24		✓	÷	✓					
	25		✓	÷	✓					
	26		✓	-	-					
	27		✓	-	-					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	11/237003.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 08:58
S2	0	60/613909.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 09:03
S3	0	11/237004.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:49
S4	1	11/237119.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:50
S5	0	11/237199.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:50
S6	15	((JAMES) near2 (ROSKIND)).INV.	USPAT	ADJ	ON	2008/11/03 16:51
S7	1	((AARON) near2 (EMIGH)).INV.	USPAT	ADJ	ON	2008/11/03 16:56
S8	120335	network near3 access	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:14
S9	73	detect$3 same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:16
S10	5527	protect near4 network	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:17
S11	80	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 10:21
S12	0	"9478944".pn.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:44
S13	0	"9478944".pn.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:44
S14	0	"10756682".app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:45
S15	1	09/478944.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:47

S16	7	"478944".ap.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:54
S17	80	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:11
S18	1	S16 and S17	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:11
S19	0	METHOD AND SYSTEM FOR PROTECTING A COMPUTER USING A REMOTE E-MAIL SCANNING DEVICE.ti.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:18
S20	1	REMOTE E-MAIL SCANNING DEVICE.ti.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:18
S21	833	kim-do-$.in.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:20
S22	2	kim-do-k.in.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:20
S23	25	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3 and (protect $3 near2 network)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/05 09:12
S24	3	quarant$3 same remediat$3 same DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/06 16:32
S25	35	quarant$3 same DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/06 16:40
S26	42	quarant$3 near3 (server or host or computer) same communicat$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:49
S27	40	quarant$3 near3 (server or host or computer) same virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:53
S28	527	quarant$3 same virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:55
S29	400	quarant$3 same virus and computer	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:57
S30	399	quarant$3 same virus and computer and system	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:57
S31	225	quarant$3 same virus and computer and system and IP	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:58
S32	31	quarant$3 same virus and remediation	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:00

S33	77	quarant$3 same (computer near3 virus)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:02
S34	252	(quarant$3 or isolat3) with (computer or server) and virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:35
S35	1345	726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:44
S36	1345	726/22.ccls. and ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:45
S37	11	726/22.ccls. and (re$1direct or allow$ or forbid$ or isolat$ or limit$) near (compromise$ or quarantine$)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:46
S38	3	726/22.ccls. and (re$1direct or allow$ or forbid$ or isolat$ or limit$) near (quarantine$)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:51
S39	9624	DNS same IP	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
S40	646	DNS same IP same redirect $3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
S41	658	DNS same IP same re$direct $3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
S42	341	DNS same IP same re$direct $3 and @ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:00
S43	686	726/22.ccls. and @ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:17
S44	32	726/22.ccls. and @ay<="2003" and quaranti $2	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:18
S45	0	scan with open near3 back $1door	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:38
S46	0	scan$4 with open near3 back $1door	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:38
S47	217	scan$4 with open near3 (back $1door or port)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:39
S48	23	scan$4 with open near3 (back $1door or port) and 726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:40
S49	0	(detect$3 near3 (open near $3 port))and scan$4 with open near3 (back$1door or port) and 726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:55

S50	0	dns with (short$time to live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
S51	0	dns same (short$time to live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
S52	13	(short$time near3 live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
S53	0	(short$time near3 live) and DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:11
S54	933	(726/23).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2008/11/07 18:31
S55	933	726/23.CCLS.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S56	0	726/23.CCLS. AND @AD<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S57	536	726/23.CCLS. AND @AY<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S58	2	"11237003"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/04/14 13:37
S60	8	(detect$4 with traffic)same remed$6 same quarant$5	US-PGPUB; USPAT	OR	ON	2009/06/25 10:13
S61	0	(cleanliness)same remed$6 same quarant$5	US-PGPUB; USPAT	OR	ON	2009/06/25 11:07
S62	21	(clean$4)same remed$6 same quarant$5	US-PGPUB; USPAT	OR	ON	2009/06/25 11:07
S63	28	(quarant$5 and (DNS or domain adj name)) and remed$5 and (ISP or (internet adj service adj provider))	US-PGPUB; USPAT	OR	ON	2009/06/26 13:52
S64	13	(quarant$5 same (DNS or domain adj name)) and remed$5	US-PGPUB; USPAT	OR	ON	2009/06/26 14:35
S65	5	S64 not S63	US-PGPUB; USPAT	OR	ON	2009/06/26 14:35
S66	497840	remediation host	US-PGPUB; USPAT	OR	ON	2009/06/26 14:44
S67	33	remediation adj (host or server)	US-PGPUB; USPAT	OR	ON	2009/06/26 14:44
S68	1945	remediation and (isolation)	US-PGPUB; USPAT	OR	ON	2009/06/26 14:52
S69	1220	remediation and (isolation) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:52

S70	4	remediation and (isolation) and (@ad<"20040927") and (web adj server)	US-PGPUB; USPAT	OR	ON	2009/06/26 14:53
S71	0	remedia@5 near5 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:55
S72	0	remed@7 near5 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:56
S73	0	remed@7 near10 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:56
S74	0	remed@7 near10 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:57
S75	75862	(re$1direct$4 web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:58
S76	75	(re$1direct$4 adj5 web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:58
S77	0	(receiv$4 adj15 (service adj2 request$4)) same re$1direct $4 same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:04
S78	0	(receiv$4 adj15 (service adj2 request$4)) same error same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:25
S79	0	(receiv$4 adj15 (service adj2 request$4)) same reply same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:26
S80	1	(receiv$4 same (service adj2 request$4)) same reply same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:26
S81	5302596	(quarantine same web $1page)\ and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:30
S82	1	(quarantine same web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:30
S83	1	(quarant$8 same web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:34
S84	5461	(quarant$8 (server or host or computer)same web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:34
S85	0	(quarant$8 near3 (server or host or computer)same web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:34

S86	2	(quarant$8 near3 (server or host or computer) same web $1site) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:35
S87	0	(quarantined$8 near3 (server or host or computer) same web$1site) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:37
S88	32	(quarantined$8 near3 (server or host or computer)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:37
S89	2	"20050131997"	US-PGPUB; USPAT	OR	ON	2009/06/26 18:07
S90	2	"20050131997" and redirect $4	US-PGPUB; USPAT	OR	ON	2009/06/26 18:07
S91	2	"20050131997" and redirect $4 and DNS and IP	US-PGPUB; USPAT	OR	ON	2009/06/26 18:37
S92	0	webpage same (short near2 time near2 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:17
S93	0	web?page same (short near3 time near3 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:18
S94	0	web?page with (short near3 time near3 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:18
S95	4	page with (short near3 time near3 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:18
S96	10	"6996845"	US-PGPUB; USPAT	OR	ON	2009/06/26 19:52
S97	37	back$1door and virus and worm and (buffer near2 (over $flow$4 or overrun$4))	US-PGPUB; USPAT	OR	ON	2009/06/26 19:55
S98	37	back$1door and virus and worm and (buffer near2 (over $flow$4 or overrun$4)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 19:56
S99	2	(Open near2 back$1door) and virus and worm and (buffer near2 (over$flow$4 or overrun$4)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 20:43
S100	2	(detect$4 with (Open near2 back$1door)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 20:44
S101	568	(detect$4 with (Open near2 port)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 20:46
S102	0	(detect$4 with (Open near2 port)) and @ad<"20090901" and (virus and worm and buffer adj3 over adj2 (flow$4 or run$4))	US-PGPUB; USPAT	OR	ON	2009/06/26 20:47
S103	57	(detect$4 with (Open near2 port)) and @ad<"20090901" and (vulnerab$5)	US-PGPUB; USPAT	OR	ON	2009/06/26 20:48

S104	2847605	"20030188194" A1	US-PGPUB; USPAT	OR	ON	2009/06/26 21:08
S105	1	"20030188194"	US-PGPUB; USPAT	OR	ON	2009/06/26 21:08
S106	115	(scan$4 with (Open near2 port)) and @ad<"20090901" and (vulnerab$5)	US-PGPUB; USPAT	OR	ON	2009/06/26 21:12
S107	24	((scan$4 with (Open near2 port)) same clos$4) and @ad<"20090901" and (vulnerab$5)	US-PGPUB; USPAT	OR	ON	2009/06/26 21:34
S108	0	(back$1door or open$1port) with inoculat$5	US-PGPUB; USPAT	OR	ON	2009/06/29 10:03
S109	0	(back$1door or open$1port) same inoculat$5	US-PGPUB; USPAT	OR	ON	2009/06/29 10:03
S110	1	"20060031673"	US-PGPUB; USPAT	OR	ON	2009/06/29 10:16
S111	2	"20050131997"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:22
S112	51423	ISP or (internet adj service adj provid?r)	US-PGPUB; USPAT	OR	ON	2009/06/29 13:30
S113	758	(ISP or (internet adj service adj provid?r) with protect$4 near3 network).ab.	US-PGPUB; USPAT	OR	ON	2009/06/29 13:31
S114	552	(ISP or (internet adj service adj provid?r) with protect$4 near3 network).ab. and @ad<"20040901"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:31
S115	0	((ISP or (internet adj service adj provid?r) with protect$4 near3 network) same (quarant$6)).ab. and @ad<"20040901"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:32
S116	5	((ISP or (internet adj service adj provid?r) with protect$4 near3 network) same (quarant$6 or inoculat$5 or isolat$6)).ab. and @ad<"20040901"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:33
S117	505	(trusted adj computing) with (trusted adj platform)	US-PGPUB; USPAT	OR	ON	2010/04/21 10:55
S118	537	(trusted adj computing) with (trusted adj platform)	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 10:55
S119	13	(trusted adj computing) with (trusted adj platform) with attestation	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 10:56
S120	0	(trusted adj computing) with (trusted adj platform) with cleanliness	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 10:59

S121	3	(trusted adj computing) with (trusted adj platform) with virus	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 10:59
S122	6	(trusted adj computing) with (trusted adj platform) with security.ab.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:01
S123	6	S122 not S121	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:01
S124	10645	(713/153-154; 726/1,26-33;709/249,389).ccls.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:05
S125	25	(713/153-154; 726/1,26-33;709/249,389).ccls. and ((trusted adj platform).ab. or (trusted adj platform).ti.)	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:06
S126	39	(713/187-188,193-194; 726/22-25).ccls. and ((trusted adj platform).ab. or (trusted adj platform).ti.)	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:12
S127	5409	TPM	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:15
S128	1023	TPM and ("713" or "726" or "380").clas.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 11:16
S129	74	(TPM or (trusted adj platform) and ("713" or "726" or "380").clas.) with (insecure or virus or (open adj port) or invalid or anomal $4 or valnerab$5 or malicious or up$1to$1date)	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 12:33
S130	39	(TPM or (trusted adj platform) and ("713" or "726" or "380").clas.) with (insecure or virus or (open adj port) or invalid or anomal $4 or valnerab$5 or malicious or up$1to$1date) and @ad<"20050927"	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/21 12:34
S145	75	bajikar.in.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 11:09
S146	34	(bajikar near2 sundeep).in.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 11:09
S147	10	(bajikar near2 sundeep).in. and TPM	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 11:09
S148	3	"20050018618"	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 15:25

S149	57119	remediat$4 host.ti.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 19:53
S150	15236	remediat$4 host.ti. and ("713" or "726" or "380").clas.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 19:54
S151	0	(remediat$4 near3 host).ti. and ("713" or "726" or "380").clas.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 19:54
S152	2	(remediat$4 near3 host).ti.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 19:54
S153	1	(remedy$4 near3 host).ti.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 20:01
S154	0	(remedy$4 near3 host).ti. and ("713" or "726" or "380").clas.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 20:02
S155	1	(remedy$4 near3 (host or computer)).ab. and ("713" or "726" or "380").clas.	US-PGPUB; USPAT; DERWENT	OR	ON	2010/04/22 20:02
S156	2	"11237003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 11:03
S157	2191	(Trusted adj2 computing)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 19:33
S158	397	(Trusted adj2 computing adj base)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 19:33
S159	63	(Trusted adj2 computing adj base) with (virus malicious code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 19:33
S160	28	(Trusted adj2 computing adj base) with (virus malicious code) and @ad<"20040927"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 19:34

S161	5	(Trusted adj2 computing adj base) with (virus malicious) and @ad<"20040927"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/07/15 19:35

7/15/2010 9:21:07 PM
C:\Documents and Settings\jsims2\My Documents\EAST\Workspaces\11237003.wsp

Web Images Videos Maps News Shopping Gmail more ▾ Sign in

Google scholar linux , trusted computing Search Advanced Scholar Search Scholar Preferences

Scholar Articles and patents 200 - 2004 include citations Results 1 - 10 of

Design and implementation of a TCG-based integrity measurement architecture
R Sailer, X Zhang, T Jaeger, L Van ... - Proceedings of the 13th ..., 2004 - portal.acm.org
... All executable content that is loaded onto the **Linux** system is measured before execution and these measurements are protected by the **Trusted** Platform Module (TPM) that is part of the **Trusted Computing** Group (TCG) standards. ...
Cited by 474 - Related articles - All 14 versions

Terra: A virtual machine-based platform for **trusted computing**
T Garfinkel, B Pfaff, J Chow, M Rosenblum, ... - ACM SIGOPS ..., 2003 - portal.acm.org
... Compatibility VMMs can run today's operating systems, such as **Linux** and Windows, and applications without modifications, un- like alternative approaches to ... One option for maintaining user privacy, proposed by the **Trusted Computing** Group, is to use a special CA, called a ...
Cited by 507 - Related articles - BL Direct - All 93 versions

Cryptography and competition policy-issues with '**trusted computing**'
R Anderson - Economics of Information Security, 2004 - Springer
... subject matter as TC, which the reader can pronounce as 'trustworthy **computing**', '**trusted computing**' or 'treacher ... of it; it will not censor your data or take away control of your **computer**. ... acute, but further reflection suggests that a competitor producing a GNU/**linux** platform running ...
Cited by 98 - Related articles - BL Direct - All 26 versions

[BOOK] **Trusted computing** platforms: TCPA technology in context
S Pearson, B Balacheff - 2003 - books.google.com
... Architectures SAP Hardware Solutions: Servers, Storage, and Networks for mySAP.com **Trusted Computing** Platforms: TCPA ... Guide Using Visual C++ and ATL Software Optimization for High Performance **Computing** Qt Programming for **Linux** and Windows 2000 ...
Cited by 187 - Related articles - All 4 versions

[HTML] **Trusted computing** frequently asked questions
R Anderson - Against TCPA. Consultado el, 2003 - cl.cam.ac.uk
... from Bruce Schneier; some controversy stirred up by Bill Thompson, who really does appear to believe that the world of **trusted computing** will be ... October 2002 saw an article in **Linux** devices on the problems TCPA may cause for embedded systems, and an article in German in ...
Cited by 43 - Related articles - Cached

Towards virtual networks for virtual machine grid **computing**
AI Sundararaj, PA Dinda - Proceedings of the 3rd conference on ..., 2004 - portal.acm.org
... In Proceedings of the USENIX Annual **Linux** Showcase and Conference (Atlanta, GA, October 2000 ... Steenkiste , Dean Sutherland, The Architecture of the Remos System, Proceedings of the 10th IEEE International Symposium on High Performance Distributed **Computing**, p.252 ...
Cited by 158 - Related articles - All 17 versions

Property-based attestation for **computing** platforms: caring about properties, not mechanisms
AR Sadeghi, C Stüble - Proceedings of the 2004 workshop on New ..., 2004 - portal.acm.org
... Even if the enforcement mechanisms of the **trusted computing** base would be highly trustworthy (eg, because it was evaluated at EAL718), the ... Applications Conventional Operating System (eg, L4−**Linux**) Application Operating System Environment Operating System Kernel ...

Ex.1002
NETSKOPE, INC. / Page 160 of 378

Cited by 198 - Related articles - All 18 versions

Reducing TCB size by using untrusted components: small kernels versus virtual-machine monit
M Hohmuth, M Peter, H Härtig, JS ... - Proceedings of the 11th ..., 2004 - portal.acm.org
... the net- work stack from an application's **trusted computing** base and use a **trusted** wrapper component to provide confidentiality and integrity. Not having to trust the network stack allows us to reuse a robust, known-to-work implementation such as FreeBSD's or **Linux's** TCP/IP **...**
Cited by 45 - Related articles - All 12 versions

Trusted Computing. Digital Rights Management, and the Fight for Copyright Control on Your **Computer**
R Roemer... - UCLA JL Tech., 2003 - litigation-essentials.lexisnexis.com
... video, in order to escape anti-circumvention liability with DMCA § 1201(f) they would have to ensure that program only worked on **Linux** and that it did not disable any of Disney's DRM controls. b. Protecting Personally Identifying Information **Trusted computing** systems must **...**
Cited by 19 - Related articles - All 2 versions

Establishing the genuinity of remote **computer** systems
R Kennell, LH Jamieson - Proceedings of the 12th conference on ..., 2003 - portal.acm.org
... ACM has opted to expose the complete List rather than only correct and linked references. 1. [1] **Trusted Computing** Platform Aliance. TCPA main specification. http://www. **trustedcomputing**.org/. **...** Design and implementation of signed executables for **linux**. **...**
Cited by 96 - Related articles - All 13 versions

Create email alert

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

linux , trusted computing Search

Go to Google Home - About Google - About Google Scholar

©2010 Google

Ex.1002
NETSKOPE, INC. / Page 161 of 378

Google scholar SUN SPARC TCB, OR TPM "trusted computir Search Advanced Scholar Search Scholar Preferences

Scholar Articles and patents 200 - 2004 include citations Results **1** - **10** of

[PDF] JVM **TCB**: Measurements of the **trusted computing** base of Java virtual machines
AW Appel, DC Wang - 2002 - cs.princeton.edu
... we estimate this size at 5,000 lines, which is the size of **Sun's** verifier [Mic01 **...** is a very rough estimate of the size of compiler, prover, and the non-**TCB** components of **...** 10 These are preliminary measurements of our **Sparc** opcode specification (600 lines) and instruction semantics **...**
Cited by 9 - Related articles - View as HTML - All 4 versions

[PDF] Integrating a **Trusted Computing** Base Extension Server and Secure Session Server into LINUX Operating System
MV Glover - 2001 - Citeseer
... It runs on Compaq Alpha AXP, **Sun SPARC** and UltraSPARC, Motorola 68000, PowerPC, PowerPC64, ARM, **...** designed to implement the concept of a **Trusted Computing** Base. **...** components are the Security Kernel, **TCB** System Services (TSS), Trusted Software, and the **...**
View as HTML - All 9 versions

[PDF] A framework on security with **trusted computing**
N Pichumani - 2004 - etd.ohiolink.edu
... 23 Page 26. Chapter 3: Security with **Trusted Computing** 3.1 Software Security: The communication channel between the vendor and the customer is secured by encrypting **...** 3. GCC The GNU C compiler generating **Sparc** Code 4. GO Artificial Intelligence plays the game Go. **...**
Related articles - View as HTML - All 8 versions

[CITATION] A metaobject architecture for fault-tolerant distributed systems: The FRIENDS appro
JC Fabre, T Pérennou - IEEE Transactions on Computers, 1998
Cited by 191 - Related articles - BL Direct - All 19 versions

[PDF] Mandatory Security Policy Enforcement in Commercial Off the Shelf Database Manageme System Software: A Comparative Analysis of Informix On-Line/ ...
KE Muschalek - 1994 - Citeseer
... the **trusted computing** base. The **trusted computing** base (**TCB**) has been defined by the the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. **...**
View as HTML - All 7 versions

Systems and methods for performing secure communications between an authorized computin platform and a hardware component
T Tahan - US Patent App. 10/986,526, 2004 - Google Patents
... 710 Lakeway Drive Sunnyvale, CA 94085 (US) (73) Assignee: **SUN** MICROSYSTEMS, INC **...** Exemplary processors include Scalable Processor Architec- ture (**SPARC**) processors, Pentium processors, PowerPC **...** the art will appreciate that trusted platform module (**TPM**) 110 may **...**
All 3 versions

A provably sound TAL for back-end optimization
J Chen, D Wu, AW Appel, H Fang - ACM SIGPLAN Notices, 2003 - portal.acm.org
... The typing rules and the type checker are in the **trusted computing** base (**TCB**), that is, bugs in these components can let unsafe code slip past the checker. **...** Compiles to a real target machine. We generate high-quality **Sparc** code. Foundational specification. **...**

Cited by 48 - Related articles - BL Direct - All 18 versions

A Study of Covert Channels in a Trusted Unix System.
RJ DeJong, NAVAL POSTGRADUATE SCHOOL ... - 1995 - oai.dtic.mil
... configuration, server support services, **SUN** hardware configuration, and local site security requirements. [Ref. 5, pp. 138-140] 10 Page 22. 2. Planning the Configuration and Installation of the Distributed System In order to preserve the **trusted computing** base (**TCB**), the closed **...**
Cited by 3 - Related articles - All 3 versions

Systems and methods for securing a computer boot
TE Tahan - US Patent App. 10/934,868, 2004 - Google Patents
... DRIVE SUITE 200 SUNNYVALE, CA 94085 (US) (73) Assignee: **SUN** MICROSYSTEMS, INC **...** For this purpose, a **TPM** that physically resides in one or more **...** Exemplary processors include Scalable Processor Architecture (**SPARC**) processors, Pentium processors, PowerPC **...**
All 3 versions

System Engineering Concept Demonstration, Security Study. Volume 7
MA Carrio Jr, SOFTWARE PRODUCTIVITY ... - 1992 - oai.dtic.mil
Page 1. AD-A265 473 RL-TR-92-345, Vol VII (of seven) Final Technical Report December 1992 SYSTEM ENGINEERING CONCEPT DEMONSTRATION, Security Study MTM Software Engineering, Inc. ; t DTIC Miguel A. Carrio, Jr. ELECTU **...**
Related articles - View as HTML - All 3 versions

Create email alert

Gooogle ▶
Result Page: 1 2 3 **Next**

SUN SPARC TCB, OR TPM "trustec Search

Go to Google Home - About Google - About Google Scholar

©2010 Google

Ex.1002
NETSKOPE, INC. / Page 163 of 378

PLUS Search Results for S/N 11237003, Searched Tue Jul 13 10:36:00 EDT 2010

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20050229250 37
20060074896 32
20070282770 32
5802151 32
6301661 31
7017181 31
7113593 31
20030016822 31
20050010801 31
20050193103 31
20050195780 31
20060156036 31
20070260649 31
5109413 31
7460946 31
20060015241 31
20070080823 31
20030163610 30
20080091538 30
20080313489 29
7592906 28
7580701 28
20050267954 28
20060230289 28
20060256730 28
20070136808 28
20070220607 28
20070255723 28
20080040785 28
6578011 27
6701453 27
7437608 27
20040039906 27
20040242973 27
20060123273 27
20080301495 27
20090181046 27
5307462 27
5392269 27
5442772 27
5528755 27
5802547 27
5832511 27
5909700 27
5974482 27
6023724 27
6154775 27
6349350 27
6469991 27
6657535 27

PLUS Search Results for S/N 11237003, Searched Tue Jul 13 10:35:55 EDT 2010

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

4261301 73
5640499 73
4514767 63
4838076 63
4914518 63
5515011 63
5756779 63
5926429 63
5963571 63
6142624 63
6236307 63
6424589 63
20050114096 63
20090199156 54
4318706 54
5755281 54
4335695 54
4357657 54
4373572 54
4437441 54
4488904 54
4532464 54
4532443 54
4585538 54
4594631 54
4812856 54
4815324 54
4820492 54
4835581 54
4864970 54
4947085 54
4953355 54
4965715 54
5003229 54
5019956 54
5184699 54
5208474 54
5208904 54
5230240 54
5248893 54
5270290 54
5285735 54
5298766 54
5317802 54
5326977 54
5345393 54
5349666 54
5367873 54
5414273 54
5452347 54

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	2437
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being electronically filed on: May 2, 2010.

/Aaron T. Emigh/

RESPONSE TO RESTRICTION REQUIREMENT

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

Dear Sir:

In response to the Restriction Requirement dated 4/26/2010, Applicant hereby elects, without traverse, group I, claims 1-2, 4-10, 12-14, and 24-25, to prosecute in the above-identified patent application.

Applicant hereby makes and generally authorizes any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed, and is given general authorization to charge any fees or to credit any overpayment during the pendency of this application, to Deposit Account No. 50-4831 (Applicant Docket No. PB-034).

Should the Examiner have any questions concerning this matter, the undersigned can be reached by telephone at 415-297-1305.

Respectfully submitted,

/Aaron T. Emigh/

Aaron Emigh
Customer #85853

Electronic Acknowledgement Receipt

EFS ID:	7532040
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	02-MAY-2010
Filing Date:	27-SEP-2005
Time Stamp:	18:19:08
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	Response to Election / Restriction Filed	PB-034-restriction-response.pdf	84495 29688f23d6d320e607b32d78a8b2f2db3ce3b2d2	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	84495

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 04/26/2010

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
04/26/2010	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.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

-- 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 *1* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2010.*

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

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-10,12-18 and 21-25* is/are pending in the application.

4a) Of the above claim(s) *3, 11, 19-20, and 26-27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the application 11/237,003 filed on 09/27/2005, and amendment filed on 01/10/2010.

Election/Restrictions

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-2, 4-10, 12-14, and 24-25, drawn to a method or system or a computer program product for protecting a network, classified in class 726, subclass 22.

II. Claim15-17, drawn to a method for processing requests from a quarantined host to communicate via a protected network, classified in class 726, subclass 27.

III. Claim 18, and 21-23, drawn to a method for remedying an insecure condition in a host associated with a protected network, classified in class 726, subclass 23 or 25.

The inventions are distinct, each from the other because of the following reasons:

3. Inventions of group I, group II, and group III are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the

independent claims 1, 9, and 14 include three elements: detecting an insecure condition, quarantining, and remediation. A method or a system or a computer program product for protecting a network is “evidence claim” which does not require the details of subcombination claim 15 or 18 for patentability. The subcombinations have separate utility such as quarantining a host and remediation a host.

The examiner has required restriction between combination and subcombination inventions. Where applicant elects a subcombination, and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

4. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and examination burden if restriction were not required because one or more of the following reasons apply:

(a) the inventions have acquired a separate status in the art in view of their different classification;

(b) the inventions have acquired a separate status in the art due to their recognized divergent subject matter;

(c) the inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

(d) the prior art applicable to one invention would not likely be applicable to another invention;

(e) the inventions are likely to raise different non-prior art issues under 35 U.S.C. 101 and/or 35 U.S.C. 112, first paragraph.

5. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and examination burden if restriction were not required because one or more of the following reasons apply:

(a) the inventions have acquired a separate status in the art in view of their different classification;

(b) the inventions have acquired a separate status in the art due to their recognized divergent subject matter;

(c) the inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

(d) the prior art applicable to one invention would not likely be applicable to another invention;

(e) the inventions are likely to raise different non-prior art issues under 35 U.S.C. 101 and/or 35 U.S.C. 112, first paragraph.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable on the elected invention.

If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

6. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one

or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. 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.

/JING SIMS/
Examiner, Art Unit 2437

/Michael Pyzocha/
Primary Examiner, Art Unit 2437

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	4148

✓	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	11/07/2008	06/29/2009	04/22/2010						
	1	✓	✓	÷						
	2	✓	✓	÷						
	3	✓	-	-						
	4	✓	✓	÷						
	5	✓	✓	÷						
	6	✓	✓	÷						
	7	✓	✓	÷						
	8	✓	✓	÷						
	9	✓	✓	÷						
	10	✓	✓	÷						
	11	✓	-	-						
	12	✓	✓	÷						
	13	✓	✓	÷						
	14	✓	✓	÷						
	15	✓	✓	÷						
	16	✓	✓	÷						
	17	✓	✓	÷						
	18	✓	✓	÷						
	19	✓	-	-						
	20	✓	-	÷						
	21		✓	÷						
	22		✓	÷						
	23		✓	÷						
	24		✓	÷						
	25		✓	÷						
	26		✓	-						
	27		✓	-						

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: January 10, 2010.

/Aaron T. Emigh/
Aaron Emigh

AMENDMENT B

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

Dear Sir:

This is in response to the Office Action mailed July 9, 2008. The following amendments and remarks are respectfully submitted.

IN THE CLAIMS

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

Listing of Claims:

1. (previously presented) A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

2. (previously presented) A method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed.

3. (canceled)

4. (original) A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.

5. (original) A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

6. (original) A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to a remediation host.

7. (original) A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.

8. (original) A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

9. (previously presented) A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and

a memory coupled to the processor and configured to provide instructions to the processor.

10. (original) A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion.

11. (canceled)

12. (previously presented) A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.

13. (original) A system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

14. (previously presented) A computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

15. (currently amended) A method for processing requests from a quarantined host to communicate via a protected network, comprising:

receiving from an operating system update service an indication that a security update is present;

establishing a quarantine, wherein establishing the quarantine comprises:

receiving a service request sent by the quarantined host;

serving a quarantine notification page to the quarantined host if the service request comprises a web server request; [[and]]

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host;

receiving from the operating system update service an assertion that no security updates are pending; and

removing the quarantine.

16. (original) A method as recited in claim 15, further comprising, in the event the service request comprises a DNS query, proxying the service request to a DNS service if the host name that is the subject of the DNS query is associated with a remediation host.

17. (original) A method as recited in claim 15, wherein providing in response an IP address of a quarantine server includes providing a response with a short time to live.

18. (previously presented) A method for remedying an insecure condition in a host associated with a protected network, comprising:

detecting an open backdoor port on the host, wherein detecting the open backdoor port includes testing the host for an existence of at least one potential backdoor associated with a security vulnerability; and

using the open backdoor port to communicate with the host as required to remedy the insecure condition.

19. (canceled)

20. (canceled)

21. (previously presented) A method as recited in claim 18, wherein the open backdoor port is associated with installation by at least one of a virus and a worm.

22. (previously presented) A method as recited in claim 18, wherein the open backdoor port is associated with a buffer overrun exploit.

23. (previously presented) A method as recited in claim 18, wherein communicating with the host as required to remedy the insecure condition includes exploiting the security vulnerability.

24. (previously presented) A method as recited in claim 1, further comprising:

receiving a service request sent by the first host;

serving a quarantine notification page to the first host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

25. (previously presented) A method as recited in claim 1, performed at an Internet service provider.

26. (canceled)

27. (canceled)

REMARKS

Claims 1, 2, 4-10, 12-18, and 21-25 are pending. Claim 15 has been amended. Claims 26 and 27 have been canceled. Support for the amendments can be found without limitation at paragraphs 53, and Figures 14-16, of the specification.

The Examiner has rejected claims 1, 2, 4-10, and 12-14 under 35 USC 102(e) as being anticipated by Liang (US 7,287,278). Applicant respectfully traverses.

Liang does not appear to teach or suggest "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness," nor "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network," as recited in amended independent claims 1 and 14, and similarly in amended independent claim 9.

Breaking down individual elements of the limitations further, the Examiner has cited Liang, column 8, lines 49-53 as anticipating "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host," as recited in claims 1, 9, and 14. However, the cited passages of Liang read "For example, virus monitor 102-1 sends a query 140 *to each of the client devices* 110-116 requesting confirmation that each has installed therein the appropriate anti-virus software as determined by the policies contained in the OPP file 135…" (Liang, column 8, lines 49-53, emphasis added.) Nothing in this, or elsewhere in Liang, appears to teach or suggest "contacting a trusted computing base," nor "a trusted computing base associated with a trusted platform module within the first host," as recited in claims 1, 9, and 14. Applicant notes that "trusted computing base" and "trusted platform module are terms of art with specific meanings that are in no way discussed in Liang. The Wikipedia entry for "Trusted Platform Module (http://en.wikipedia.org/wiki/Trusted_platform_module; retrieved January 10, 2010) begins, "In

computing, Trusted Platform Module (TPM) is both the name of a published specification detailing a secure cryptoprocessor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device" (as designated in certain Dell BIOS settings[1]). The TPM specification is the work of the Trusted Computing Group. The current version of the TPM specification is 1.2 Revision 103, published on July 9, 2007." Reinforcing the industry adoption of this technology and standardization around the term of art used in the claims, this specification has also been adopted as ISO/IEC standard 11889. As for the term of art "trusted computing base," the final paragraph of the "Definition and characterization" section of the Wikipedia entry on "Trusted Computing Base" (http://en.wikipedia.org/wiki/Trusted_computing_base; retrieved January 10, 2010) states that "A given piece of hardware or software is a part of the TCB if and only if it has been designed to be a part of the mechanism that provides its security to the computer system."

Liang does not appear to teach or suggest a trusted platform module, nor a trusted computing base associated with a trusted platform module. Indeed, Applicant discussed the previously presented amendment to claims 1, 9, and 14 with the Examiner and Supervisory Patent Examiner Emmanuel Moise on April 14, 2009. During that interview, the Examiner explicitly stated that she believed the language in these claims as amended in Amendment A and presented herein overcame Liang, as indeed, they appear to do.

Similarly, the Examiner has cited Liang, column 8, lines 53-55 as anticipating "determining whether the response includes a valid digitally signed attestation of cleanliness." The cited section of Liang reads "Upon receiving the query 140, each of the client devices checks for confirmation that the appropriate anti-virus software is indeed present." This, as elsewhere in Liang, does not appear to teach or suggest a "valid digitally signed attestation of cleanliness."

Similarly, the Examiner has cited Liang, column 8, lines 55-59 as anticipating "when it is determined that the response does not include a valid digitally signed attestation of cleanliness." The cited section of Liang reads "If, say in the case of the client device 116, that [sic] it is determined that either no software is present or the installed software is not appropriate (based upon the policies of the OPP file 135, for example), the client device 116 is directed only to the anti-virus software installation server 138 and no other..." This, as elsewhere in Liang, does not appear to teach or suggest a "valid digitally signed attestation of cleanliness."

The use of a trusted computing base, trusted platform module, and valid digitally signed attestation of cleanliness in detecting an insecure condition are significant innovations, as they can, for example, prevent false reports by ensuring that an attestation of cleanliness is reliable and the result of properly executed checks. Without the use of such techniques, approaches such as Liang are potentially vulnerable to false reports by infected machines, and may fail to quarantine such machines, resulting in higher infection rates and greater propagation of malicious software.

Claims 1, 9, and 14 are therefore believed to be allowable.

Claims 2 and 4-8 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claims 10, 12, and 13 depend from claim 9 and are believed to be allowable for the same reasons described above.

The Examiner has rejected claims 15, 16, and 26 under 35 USC 102(e) as being anticipated by Lewis et al (US Pub. No. 2005/0131997 A1), hereinafter referred to as Lewis.

Lewis does not appear to teach or suggest "receiving from an operating system update service an indication that a security update is present," nor "receiving from the operating system update service an assertion that no security updates are pending; and removing the quarantine," as recited in amended claim 15.

Claim 16 depends from claim 15 and is believed to be allowable for the same reasons described above. Claim 26 has been canceled.

The Examiner has rejected claim 24 under 35 USC 103(a) as being unpatentable over Liang in view of Lewis.

Neither Liang nor Lewis, alone or in combination, appear to teach or suggest "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness," nor "when it is determined that the response does not include a valid digitally signed attestation of

cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network," as recited in amended independent claim 1.

Claim 24 depends from claim 1 and is believed to be allowable for the same reasons described above.

The Examiner has rejected claim 25 under 35 USC 103(a) as being unpatentable over Liang in view of McElhaney, Jr., et al (US Patent No. 6,823,479 B1), hereinafter referred to as McElhaney.

Neither Liang nor McElhaney, alone or in combination, appear to teach or suggest "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness," nor "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network," as recited in amended independent claim 1.

Claim 25 depends from claim 1 and is believed to be allowable for the same reasons described above.

The Examiner has rejected claim 17 under 35 USC 103(a) as being unpatentable over Lewis in view of Andreev et al (US Pub. No. 2005/0182817 A1), hereinafter referred to as Andreev.

Neither Lewis nor Andreev, alone or in combination, appear to teach or suggest "receiving from an operating system update service an indication that a security update is present," nor "receiving from the operating system update service an assertion that no security updates are pending; and removing the quarantine," as recited in amended claim 15.

Claim 17 depends from claim 15 and is believed to be allowable for the same reasons described above.

The Examiner has rejected claim 27 under 35 USC 103(a) as being unpatentable over Lewis in view of McElhaney.

Claim 27 has been canceled.

The Examiner has rejected claims 18 and 21-23 under 35 USC 103(a) as being unpatentable over Mualem et al (US Pub. No. 2005/0018618 A1), hereinafter referred to as Mualem, in view of Bohra et al, "Remote Repair of Operating System State Using Backdoors," hereinafter referred to as Bohra. Applicant respectfully traverses.

Neither Mualem nor Bohra, alone or in combination, appear to teach or suggest "detecting an open backdoor port on the host, wherein detecting the open backdoor port includes testing the host for an existence of at least one potential backdoor associated with a security vulnerability," nor "using the open backdoor port to communicate with the host as required to remedy the insecure condition," as recited in independent claim 18.

The Examiner has cited Mualem, paragraphs 57-67, as anticipating "detecting an open backdoor port on the host, wherein detecting the open backdoor port includes testing the host for an existence of at least one potential backdoor associated with a security vulnerability." As a rationale, the Examiner has characterized these paragraphs as teaching "different port scan method to find the vulnerabilities of a host." Applicant respectfully notes that finding a vulnerability is different from detecting an open backdoor port, and furthermore that in fact, the cited paragraphs of Mualem appear to teach *detection* of port scanning, not *implementation* of scanning for an open backdoor port. For example, in the paragraphs cited by the Examiner: "The *port scan detection* module in step S50 *detects port scans* using a trending cache" (Mualem, paragraph 57, emphasis added); "The scans that the *port scan detection* module can detect include, but are not limited to:" (Mualem, paragraph 58, emphasis added; followed by the methods noted by the Examiner).

The Examiner has cited Bohra, as disclosing "using the open backdoor port to communicate with the host as required to remedy the insecure condition." However, Bohra appears not to discuss backdoors in the sense used in the instant application, i.e. as a term of art, but rather discusses "Backdoors" as the name of their research project ("Backdoors is a novel system architecture that enables remote monitoring…," Bohra, Abstract) and "backdoor" as a

programmable network interface card used in this project ("The core of the architecture is the *backdoor*, a programmable NIC placed on the system I/O bus…," Bohra, page 2, section 2, first paragraph, emphasis in original). By way of contrast, the Wikipedia entry for "Backdoor" discussing the standard usage of the term among those skilled in the art, retrieved January 10, 2010 from http://en.wikipedia.org/wiki/Backdoor_%28computing%29, begins "A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device." Applicant therefore believes that discussion in Bohra of "backdoors" and a "backdoor" as cited by the Examiner is not necessarily relevant to the instant application, as Bohra has adopted non-standard definitions of those terms of art.

Independent claim 18 is therefore believed to be allowable.

Claims 21-23 depend from claim 18 and are believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: January 10, 2010

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

PETITION FOR EXTENSION OF TIME AND AUTHORIZATION TO CHARGE FEES DURING PENDENCY OF APPLICATION

Applicant hereby petitions for an extension of time in which to respond to the outstanding Office Action, within the third month. Since the day that is six months after the mailing date of the office action (e.g. within the third month of the extension period) to which this amendment is responsive falls on a Saturday, Sunday, or Federal holiday, per 35 USC section 1.7, this amendment is being filed before the next succeeding business day.

Applicant hereby makes and generally authorizes any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed, and is given general authorization to charge any fees or to credit any overpayment during the pendency of this application, to Deposit Account No. 50-4831 (Applicant Docket No. PB-034).

Electronic Patent Application Fee Transmittal

Application Number:	11237003
Filing Date:	27-Sep-2005
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-034

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	2253	1	555	555

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**555**

Electronic Acknowledgement Receipt

EFS ID:	6781152
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	10-JAN-2010
Filing Date:	27-SEP-2005
Time Stamp:	23:53:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$555
RAM confirmation Number	6598
Deposit Account	504831
Authorized User	

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		PB-034-amendment-b.pdf	124862 95394ff13e1b7af2bc2117e961fd6812e076b28b	yes	12

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	11
Extension of Time	12	12

Warnings:

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	29509 2facc0a4c9404289465b58ca09b4a493b3d6fd5	no	2

Warnings:

Information:

Total Files Size (in bytes):	154371

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/237,003	Filing Date 09/27/2005	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	01/10/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 21	Minus	** 23	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 5	Minus	***5	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/JACQUELINE E. COUPLIN/

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.

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

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Radix Holdings, LLC

Application No./Patent No.: 11/237,003 Filed/Issue Date: 9/27/2005

Titled: CONTAGION ISOLATION AND INOCULATION

Radix Holdings, LLC , a Nevada Limited Liability Company
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

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

1. From: Aaron Emigh, James Roskind, and Radix Labs, LLC To: Aaron Emigh
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

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

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

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

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

/ Aaron T. Emigh / October 24, 2009
Signature Date

Aaron Emigh President and Manager
Printed or Typed Name Title

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

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

ASSIGNMENT OF PATENT APPLICATION

Whereas we the undersigned inventors have invented certain new and useful improvements as set forth in the patent application entitled:

CONTAGION ISOLATION AND INOCULATION

for which we have executed an application for a United States Letters Patent which was filed in the U.S. Patent and Trademark Office on September 27, 2005, and which bears the Application No. 11/237003;

We the undersigned inventor(s) and managers of Radix Labs, LLC, pursuant to the Amended Judgment entered in *Roskind v. Emigh et al.*, Case No. CV-S-05-00825-RCJ-RJJ on August 14, 2009, and subject to the Joint Settlement Statement on file therein, hereby:

1) Sell, assign and transfer to Aaron Emigh (hereinafter referred to as "ASSIGNEE"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) (including related foreign applications) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application.

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

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

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

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

Signed on the date(s) indicated beside our signatures.

9/11/2009
James A. Roskind Date

10/1/2009
Aaron T. Emigh Date

Radix Labs, LLC

By: 9/11/2009
James A. Roskind, Manager Date

By: 10/1/2009
Aaron T. Emigh, Manager Date

LIONEL SAWYER & COLLINS
ATTORNEYS AT LAW
1700 BANK OF AMERICA PLAZA
300 SOUTH FOURTH ST.
LAS VEGAS,
NEVADA 89101
(702) 383-8888

PATENT ASSIGNMENT

Aaron Emigh, a resident of the State of Nevada having an address at 762 Judith Court, Incline Village, NV, ("Seller"), certifies that to the best of Seller's knowledge and belief he is the sole assignee of United States Patent Application No. 11/237,003, filed September 27, 2005, entitled CONTAGION ISOLATION AND INOCULATION.

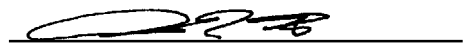
Seller hereby:

1) Assigns and transfers to Radix Holdings, LLC, a Nevada Limited Liability Company having a place of business at 762 Judith Court, Incline Village, NV ("Buyer"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) (including foreign applications) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application and/or in any provisional application to which the above referenced application claims priority.

2) Authorizes and requests the Commissioner of Patents to issue any and all Letters Patents resulting from patent applications claiming priority to or otherwise related to the above referenced patent application, including any divisional(s), continuation(s), substitutes(s) or reissue(s) thereof to Buyer.

Signed on the date indicated below my signature.

Seller

By 

Aaron Emigh
October 11, 2009

Electronic Acknowledgement Receipt

EFS ID:	6325678
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	25-OCT-2009
Filing Date:	27-SEP-2005
Time Stamp:	02:29:45
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(b).	PB-034-assignment-statement-1.pdf	356582 734f1f244855e5889311f2a986127aacbacb908	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	356582

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

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

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Radix Holdings, LLC

Application No./Patent No.: 11/237,003 Filed/Issue Date: 9/27/2005

Titled: CONTAGION ISOLATION AND INOCULATION

Radix Holdings, LLC , a Nevada Limited Liability Company
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

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

1. From: _____ To: Aaron Emigh

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: Aaron Emigh To: Radix Holdings, LLC

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

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

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

/ Aaron T. Emigh / October 14, 2009
Signature Date

Aaron Emigh President and Manager
Printed or Typed Name Title

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

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

ASSIGNMENT OF PATENT APPLICATION

Whereas we the undersigned inventors have invented certain new and useful improvements as set forth in the patent application entitled:

CONTAGION ISOLATION AND INOCULATION

for which we have executed an application for a United States Letters Patent which was filed in the U.S. Patent and Trademark Office on September 27, 2005, and which bears the Application No. 11/237003;

We the undersigned inventor(s) and managers of Radix Labs, LLC, pursuant to the Amended Judgment entered in *Roskind v. Emigh et al.*, Case No. CV-S-05-00825-RCJ-RJJ on August 14, 2009, and subject to the Joint Settlement Statement on file therein, hereby:

1) Sell, assign and transfer to Aaron Emigh (hereinafter referred to as "ASSIGNEE"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) (including related foreign applications) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application.

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

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

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

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

Signed on the date(s) indicated beside our signatures.

9/11/2009
James A. Roskind Date

10/1/2009
Aaron T. Emigh Date

Radix Labs, LLC

By: 9/11/2009
James A. Roskind, Manager Date

By: 10/1/2009
Aaron T. Emigh, Manager Date

LIONEL SAWYER & COLLINS
ATTORNEYS AT LAW
1700 BANK OF AMERICA PLAZA
300 SOUTH FOURTH ST.
LAS VEGAS,
NEVADA 89101
(702) 383-8888

PATENT ASSIGNMENT

Aaron Emigh, a resident of the State of Nevada having an address at 762 Judith Court, Incline Village, NV, ("Seller"), certifies that to the best of Seller's knowledge and belief he is the sole assignee of United States Patent Application No. 11/237,003, filed September 27, 2005, entitled CONTAGION ISOLATION AND INOCULATION.

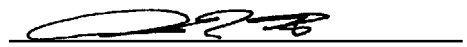
Seller hereby:

1) Assigns and transfers to Radix Holdings, LLC, a Nevada Limited Liability Company having a place of business at 762 Judith Court, Incline Village, NV ("Buyer"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) (including foreign applications) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application and/or in any provisional application to which the above referenced application claims priority.

2) Authorizes and requests the Commissioner of Patents to issue any and all Letters Patents resulting from patent applications claiming priority to or otherwise related to the above referenced patent application, including any divisional(s), continuation(s), substitutes(s) or reissue(s) thereof to Buyer.

Signed on the date indicated below my signature.

Seller

By 

Aaron Emigh
October 11, 2009

Electronic Acknowledgement Receipt

EFS ID:	6257272
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	14-OCT-2009
Filing Date:	27-SEP-2005
Time Stamp:	02:31:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73(b).	PB-034-assignment-statement.pdf	169821 89ea2631e65aa5d529f56680cb98369c36416083	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	169821

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 07/09/2009

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
07/09/2009	PAPER

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

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *4/14/2009.*

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

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) *3, 11, 19, and 20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4-10, 12-18, 20-27* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application 11/237,003, filed on 9/27/2005; amendment filed on 4/14/2009.

2. Claims 1, 2, 9, 12, 14, and 18 are amended. New claims 21-27 have been added. Claims 3, 11, 19, and 20 have been canceled

3. Applicant's arguments, with respect to claims 15-17 of the non-final rejection of the last Office action is persuasive and, therefore, non-final of that action is withdrawn.

Claim Rejections - 35 USC § 102

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

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

5. <u>Claims 1, 2, 4-10, and 12-14</u> are rejected under 35 U.S.C. 102(e) as being anticipated by Liang (US 7287278 B2).

As per claim 1, Liang discloses "a method for protecting a network, comprising":

"detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present), "quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line

61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

As per claim 2, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 4, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes 20 determining that the first host should be quarantined until an update to an operating system has been installed" (col. 8 line 55-64, if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 5, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system" (col. 17, line 47-55, identifying a new client device to e added to the network. Identification includes identifying the type of system, resident operating system etc. In col. 18, line 4-7, if the new client has been determined that proper anti-virus policies and protocols are not in place, then all access to all addresses except to that of an anti-virus software installation server are blocked. Liang teaches the client need to meet certain safety policies and protocols to access the network. The initial startup after installation of the operating system is the configuration of the system; therefore, it is the policies and protocols).

As per claim 6, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular those data packets found to be virus-free are sent back to the network traffic flow).

As per claim 7, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular data packets deemed more likely to be affected are passed directly to the file scan module. A data packet is always has its purpose to request service from the destination network and it is usually not address to a remediation host).

As per claim 8, Liang discloses "a method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 9, Liang discloses “a system for protecting a network, comprising: a processor configured to”:

“detect an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor monitors activities of network, detecting abnormal events from other computers that on the network. Liang also describes virus monitors can be a stand alone server computer in col. 7, line 15-21), “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host” (col. 8, lines 49-53, send a query to client device requesting confirmation);

“and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)”;

“when it is determined that the response does not include a valid digitally signed attestation of cleanliness” (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"and permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak) "and a memory coupled to the processor and configured to provide instructions to the processor" (col. 7, line 15-21, virus monitors can be a stand alone server computer. Every stand alone computer includes memory and processor).

As per claim 10, Liang discloses “a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data” (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) “checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion” (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 12, Liang discloses "a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed" (col. 7, line 25-36, the controller includes a rules engine used to store and source of detection rules for detecting computer viruses and an outbreak prevention policy distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak. Liang also discloses the policies, protocols and procedures can be periodically updated. Checking initial startup after installation of an OS is regular procedure to perform for securing of a computer, therefore the rules, polices, or procedures that Liang described include that checking initial startup after installation of an OS).

As per claim 13, Liang discloses "a system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 14, Liang discloses "a computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for" (col. 3, line 44-45, and line 59-67, a computer program project for monitoring a network for computer viruses):

"detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems);

"and permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

6. Claims 15, 16, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Lewis et al. (US Publication No. US 2005/0131997 A1) (hereinafter Lewis).

As per claim 15, Lewis discloses "a method for processing requests from a quarantined host to communicate via a protected network, comprising:

receiving a service request sent by the quarantined host; serving a quarantine notification page to the quarantined host if the service request comprises a web server request" (page 8, [0083], lines 20-22, wherein a quarantine notification page corresponding to fix-up page on QS, QS stands for quarantine server);

"and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host" (page 8, [0082], the purpose is to prevent the unsafe machine from talking to any other network node except for the few select severs it can use to update it compliance with network security policy; [0083], whenever the client performs name resolution on any address, it will receive the IP of quarantine server. This way any client will be redirected to fix-up page on quarantine server).

As per claim 16, Lewis also discloses "a method as recited in claim 15, further comprising, in the event the service request comprises a DNS query, proxying the service request to a DNS service if the host name that is the subject of the DNS query is associated with a remediation host" (page 8, [0083], to allow connectivity to servers for getting corporate security policy manifest to the quarantine agent, updating the client with latest settings, etc).

As per claim 26, Lewis discloses "a method as recited in claim 15, further comprising:

detecting an insecure condition on the quarantined host that has connected or is attempting to connect to a protected network" (page 2, [0017], provides a system for ensuring that machines have invalid or corrupt states are restricted from accessing network resources);

quarantining the first host (page 2, [0018], the client is placed in quarantine);

and permitting the first host to communicate with the remediation host" (page 2, [0018], the only network resources accessible to the client are those necessary to install the quarantine agent and requisite software/patches).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of Lewis.

As per claim 24, Liang discloses claim 1, however, not the rest of the claim. Lewis discloses "a method as recited in claim 1, further comprising:

receiving a service request sent by the first host; serving a quarantine notification page to the first host if the service request comprises a web server request" (page 8, [0083], lines 20-22, wherein a quarantine notification page corresponding to fix-up page on QS, QS stands for quarantine server);

"and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host" (page 8, [0082], the purpose is to prevent the unsafe machine from talking to any other network node except for the few select severs it can use to update it compliance with network security policy; [0083], whenever the client performs name resolution on any address, it will receive the IP of quarantine server. This way any client will be redirected to fix-up page on quarantine server).

Liang and Lewis are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host as described by Liang and add the host request service including DNS and other requests as taught by Lewis because it would be added more detailed of the normal services that request from a host to a server in a secured network.

9. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of McElhaney, Jr. et al. (US patent no. US 6,823,479 B1) (hereinafter McElhaney).

As per claim 25, Liang discloses a method as recited in claim 1, however, not "performed at an Internet service provider".

McElhaney discloses “performed at an Internet service provider” (col. 1, line 26-35, ISP provides test tools to protect subscribers by isolate the damaged root).

Liang and McElhaney are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host in a distributed network as described by Liang and add the distributed network also can an ISP as taught by McElhaney because it would be logically expanded the network to an distributed network work such as an Internet Service Provider.

10. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Andreev et al. (US Patent Publication no. US 2005/0182817 A1).

As per claim 17, Lewis also discloses “a method as recited in claim 15”, however Lewis does not explicitly disclose “wherein providing in response an IP address of quarantine serve includes providing a response with a short time to live” .

Andreev discloses set a short time to live in the header of HTML pages in cache (page 2, [0023]).

Lewis and Andreev are analogous art because of they are from the same field of endeavor of communication on the Internet.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the response page as described by Lewis and add setting a short time to live on the page as taught by Andreev because it would improved the timely delivery of message (see Andreev, page 2, [0023]).

11. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of McElhaney.

As per claim 27, a method as recited in claim 15, performed at an Internet service provider.

Lewis and McElhaney are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host in a distributed network as described by Lewis and add the distributed network also can an ISP as taught by McElhaney because it would be logically expanded the network to an distributed network work such as an Internet Service Provider.

12. Claims 18, and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mualem et al. (US Patent Publication no. 2005/0018618 A1) (hereinafter Mualem) in view of Bohra et al. (Remote Repair of Operating System State Using Backdoors) (hereinafter Bohra).

As per claim 18, Mualem discloses “a method for remedying an insecure condition in a host associated with a protected network, comprising:

detecting an open backdoor port on the host, wherein detecting an open backdoor port on the host includes testing the host for an existence of at least one potential backdoor associated with security vulnerability” (page 6, [0057]-[0067], different port scan method to find the vulnerabilities of a host).

However, Mualem does not explicitly disclose “using the open backdoor port to communicate with the host as required to remedy the insecure condition”. Bohra discloses “using the open backdoor port to communicate with the host as required to remedy the insecure condition” (page 1, under introduction section, the paragraph starting with remote healing).

Mualem and Bohra are analogous art because of they are from the same field of endeavor of preventing attacks through system backdoors.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the port scan detection module as described by Mualem and add the remote repairing with backdoor as taught by Bohra because it would have achieved robust detection and reaction to anomalies, and enabled remote healing (see Bohra, page 1, left col., lines 3 to 1 from the bottom, and right col., Line 1).

As per claim 21, Bohra discloses “wherein the open backdoor port is associated with installation by at least one of a virus and a worm” (under section Security, para. starting with using backdoors in remote repair…).

As per claim 22, Bohra discloses “a method as recited in claim 18, wherein the open backdoor port is associated with a buffer overrun exploit” (under section 3.1. Monitoring with Sensor Box, para. starting with level sensors).

As per claim 23, Bohra discloses “a method as recited in claim 18, wherein communicating with the host as required to remedy the insecure condition includes exploiting the security vulnerability” (under section Security, para. starting with using backdoors in remote repair…).

Response to Amendment

13. On page 8 of the Applicants’ Response, Applicants have argued that Liang does not appear to teach claims 1-14. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

14. On page 10 of the Applicants’ Response, Applicants have argued that Hurst does not appear to teach "using the open backdoor port to communicate with the host as required to remedy the insecure condition" in claim 18 and 20. In this Office action, the rejection to claim 18 - claim 20 is canceled - is by Mualem in view of Bohra; therefore, the arguments are moot.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is

(571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. 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.

/JING SIMS/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/237,003	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner JING SIMS	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0131997	06-2005	Lewis et al.	709/203
*	B	US-6,823,479	11-2004	McElhaney et al.	714/43
*	C	US-2005/0018618	01-2005	Mualem et al.	370/252
	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	Bohra, A.; Neamtiu, I.; Gallard, P.; Sultan, F.; Iftode, L.; Remote repair of operating system state using Backdoors; Autonomic Computing, 2004. Proceedings. International Conference on 17-18 May 2004 Page(s):256 - 263.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	4148

✓	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	11/07/2008	06/29/2009							
	1	✓	✓							
	2	✓	✓							
	3	✓	-							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	-							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	-							
	20	✓	-							
	21		✓							
	22		✓							
	23		✓							
	24		✓							
	25		✓							
	26		✓							
	27		✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	Art Unit
	JING SIMS	4148

SEARCHED			
Class	Subclass	Date	Examiner
726	22,23	11/3/2008	JS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in EAST	11/7/2008	JS
Text Search (see EAST notes)	11/7/2008	JS
Updated EAST Search	6/29/2009	JS
Google Patent Search	6/29/2009	JS
Google Scholar Search	6/29/2009	JS
IEEE Search	6/29/2009	JS

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	11/237003.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 08:58
S2	0	60/613909.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 09:03
S3	0	11/237004.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:49
S4	1	11/237119.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:50
S5	0	11/237199.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:50
S6	15	((JAMES) near2 (ROSKIND)).INV.	USPAT	ADJ	ON	2008/11/03 16:51
S7	1	((AARON) near2 (EMIGH)).INV.	USPAT	ADJ	ON	2008/11/03 16:56
S8	120335	network near3 access	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:14
S9	73	detect$3 same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:16
S10	5527	protect near4 network	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:17
S11	80	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 10:21
S12	0	"9478944".pn.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:44
S13	0	"9478944".pn.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:44
S14	0	"10756682".app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:45
S15	1	09/478944.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:47
S16	7	"478944".ap.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:54

S17	80	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:11
S18	1	S16 and S17	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:11
S19	0	METHOD AND SYSTEM FOR PROTECTING A COMPUTER USING A REMOTE E-MAIL SCANNING DEVICE.ti.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:18
S20	1	REMOTE E-MAIL SCANNING DEVICE.ti.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:18
S21	833	kim-do-$.in.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:20
S22	2	kim-do-k.in.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:20
S23	25	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3 and (protect $3 near2 network)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/05 09:12
S24	3	quarant$3 same remediat$3 same DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/06 16:32
S25	35	quarant$3 same DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/06 16:40
S26	42	quarant$3 near3 (server or host or computer) same communicat$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:49
S27	40	quarant$3 near3 (server or host or computer) same virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:53
S28	527	quarant$3 same virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:55
S29	400	quarant$3 same virus and computer	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:57
S30	399	quarant$3 same virus and computer and system	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:57
S31	225	quarant$3 same virus and computer and system and IP	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:58
S32	31	quarant$3 same virus and remediation	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:00
S33	77	quarant$3 same (computer near3 virus)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:02

S34	252	(quarant$3 or isolat3) with (computer or server) and virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:35
S35	1345	726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:44
S36	1345	726/22.ccls. and ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:45
S37	11	726/22.ccls. and (re$1direct or allow$ or forbid$ or isolat$ or limit$) near (compromise$ or quarantine$)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:46
S38	3	726/22.ccls. and (re$1direct or allow$ or forbid$ or isolat$ or limit$) near (quarantine$)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:51
S39	9624	DNS same IP	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
S40	646	DNS same IP same redirect $3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
S41	658	DNS same IP same re$direct $3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
S42	341	DNS same IP same re$direct $3 and @ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:00
S43	686	726/22.ccls. and @ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:17
S44	32	726/22.ccls. and @ay<="2003" and quaranti $2	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:18
S45	0	scan with open near3 back $1door	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:38
S46	0	scan$4 with open near3 back $1door	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:38
S47	217	scan$4 with open near3 (back $1door or port)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:39
S48	23	scan$4 with open near3 (back $1door or port) and 726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:40
S49	0	(detect$3 near3 (open near $3 port))and scan$4 with open near3 (back$1door or port) and 726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:55
S50	0	dns with (short$time to live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10

S51	0	dns same (short$time to live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
S52	13	(short$time near3 live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
S53	0	(short$time near3 live) and DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:11
S54	933	(726/23).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2008/11/07 18:31
S55	933	726/23.CCLS.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S56	0	726/23.CCLS. AND @AD<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S57	536	726/23.CCLS. AND @AY<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S58	2	"11237003"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/04/14 13:37
S60	8	(detect$4 with traffic)same remed$6 same quarant$5	US-PGPUB; USPAT	OR	ON	2009/06/25 10:13
S61	0	(cleanliness)same remed$6 same quarant$5	US-PGPUB; USPAT	OR	ON	2009/06/25 11:07
S62	21	(clean$4)same remed$6 same quarant$5	US-PGPUB; USPAT	OR	ON	2009/06/25 11:07
S63	28	(quarant$5 and (DNS or domain adj name)) and remed$5 and (ISP or (internet adj service adj provider))	US-PGPUB; USPAT	OR	ON	2009/06/26 13:52
S64	13	(quarant$5 same (DNS or domain adj name)) and remed$5	US-PGPUB; USPAT	OR	ON	2009/06/26 14:35
S65	5	S64 not S63	US-PGPUB; USPAT	OR	ON	2009/06/26 14:35
S66	497840	remediation host	US-PGPUB; USPAT	OR	ON	2009/06/26 14:44
S67	33	remediation adj (host or server)	US-PGPUB; USPAT	OR	ON	2009/06/26 14:44
S68	1945	remediation and (isolation)	US-PGPUB; USPAT	OR	ON	2009/06/26 14:52
S69	1220	remediation and (isolation) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:52
S70	4	remediation and (isolation) and (@ad<"20040927") and (web adj server)	US-PGPUB; USPAT	OR	ON	2009/06/26 14:53

S71	0	remedia@5 near5 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:55
S72	0	remed@7 near5 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:56
S73	0	remed@7 near10 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:56
S74	0	remed@7 near10 (web adj2 (server or page)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:57
S75	75862	(re$1direct$4 web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:58
S76	75	(re$1direct$4 adj5 web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 14:58
S77	0	(receiv$4 adj15 (service adj2 request$4)) same re$1direct $4 same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:04
S78	0	(receiv$4 adj15 (service adj2 request$4)) same error same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:25
S79	0	(receiv$4 adj15 (service adj2 request$4)) same reply same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:26
S80	1	(receiv$4 same (service adj2 request$4)) same reply same (web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:26
S81	5302596	(quarantine same web $1page)\ and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:30
S82	1	(quarantine same web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:30
S83	1	(quarant$8 same web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:34
S84	5461	(quarant$8 (server or host or computer)same web$1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:34
S85	0	(quarant$8 near3 (server or host or computer)same web $1page) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:34
S86	2	(quarant$8 near3 (server or host or computer) same web $1site) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:35

S87	0	(quarantined$8 near3 (server or host or computer) same web$1site) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:37
S88	32	(quarantined$8 near3 (server or host or computer)) and (@ad<"20040927")	US-PGPUB; USPAT	OR	ON	2009/06/26 15:37
S89	2	"20050131997"	US-PGPUB; USPAT	OR	ON	2009/06/26 18:07
S90	2	"20050131997" and redirect $4	US-PGPUB; USPAT	OR	ON	2009/06/26 18:07
S91	2	"20050131997" and redirect $4 and DNS and IP	US-PGPUB; USPAT	OR	ON	2009/06/26 18:37
S92	0	webpage same (short near2 time near2 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:17
S93	0	web?page same (short near3 time near3 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:18
S94	0	web?page with (short near3 time near3 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:18
S95	4	page with (short near3 time near3 liv$4)	US-PGPUB; USPAT	OR	ON	2009/06/26 19:18
S96	10	"6996845"	US-PGPUB; USPAT	OR	ON	2009/06/26 19:52
S97	37	back$1door and virus and worm and (buffer near2 (over $flow$4 or overrun$4))	US-PGPUB; USPAT	OR	ON	2009/06/26 19:55
S98	37	back$1door and virus and worm and (buffer near2 (over $flow$4 or overrun$4)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 19:56
S99	2	(Open near2 back$1door) and virus and worm and (buffer near2 (over$flow$4 or overrun$4)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 20:43
S100	2	(detect$4 with (Open near2 back$1door)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 20:44
S101	568	(detect$4 with (Open near2 port)) and @ad<"20090901"	US-PGPUB; USPAT	OR	ON	2009/06/26 20:46
S102	0	(detect$4 with (Open near2 port)) and @ad<"20090901" and (virus and worm and buffer adj3 over adj2 (flow$4 or run$4))	US-PGPUB; USPAT	OR	ON	2009/06/26 20:47
S103	57	(detect$4 with (Open near2 port)) and @ad<"20090901" and (vulnerab$5)	US-PGPUB; USPAT	OR	ON	2009/06/26 20:48
S104	2847605	"20030188194" A1	US-PGPUB; USPAT	OR	ON	2009/06/26 21:08
S105	1	"20030188194"	US-PGPUB; USPAT	OR	ON	2009/06/26 21:08

S106	115	(scan$4 with (Open near2 port)) and @ad<"20090901" and (vulnerab$5)	US-PGPUB; USPAT	OR	ON	2009/06/26 21:12
S107	24	((scan$4 with (Open near2 port)) same clos$4) and @ad<"20090901" and (vulnerab$5)	US-PGPUB; USPAT	OR	ON	2009/06/26 21:34
S108	0	(back$1door or open$1port) with inoculat$5	US-PGPUB; USPAT	OR	ON	2009/06/29 10:03
S109	0	(back$1door or open$1port) same inoculat$5	US-PGPUB; USPAT	OR	ON	2009/06/29 10:03
S110	1	"20060031673"	US-PGPUB; USPAT	OR	ON	2009/06/29 10:16
S111	2	"20050131997"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:22
S112	51423	ISP or (internet adj service adj provid?r)	US-PGPUB; USPAT	OR	ON	2009/06/29 13:30
S113	758	(ISP or (internet adj service adj provid?r) with protect$4 near3 network).ab.	US-PGPUB; USPAT	OR	ON	2009/06/29 13:31
S114	552	(ISP or (internet adj service adj provid?r) with protect$4 near3 network).ab. and @ad<"20040901"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:31
S115	0	((ISP or (internet adj service adj provid?r) with protect$4 near3 network) same (quarant$6)).ab. and @ad<"20040901"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:32
S116	5	((ISP or (internet adj service adj provid?r) with protect$4 near3 network) same (quarant$6 or inoculat$5 or isolat$6)).ab. and @ad<"20040901"	US-PGPUB; USPAT	OR	ON	2009/06/29 13:33

6/29/2009 3:44:52 PM
C:\Documents and Settings\jsims2\My Documents\EAST\Workspaces\11237003.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 04/17/2009

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
04/17/2009	PAPER

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

The time period for reply, if any, is set in the attached communication.

Interview Summary	Application No.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Aaron Emigh.* (3)*Jing Sims.*

(2) *Emmanuel Moise.* (4)____.

Date of Interview: *14 April 2009.*

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *1, 3, and 15.*

Identification of prior art discussed: *US Patent No.: US 7,287,278 B2.*

Agreement with respect to the claims f)☒ was reached. g)☐ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *inventor discussed claims 1, 3, and 15 and the cited prior art with examiners. Inventor had proposed amendment to claim 3 and move claim 3 up to claim 1. Examiner has acknowledged the prior art does not explicitly teach the limitations in claim 15 at the cited paragraphs, but not the prior art as whole. Further consideration and/or updated searches of the amendment, when filed, would be necessary before any determination can be made.*

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/JING SIMS/ Examiner, Art Unit 2437	/Emmanuel L. Moise/ Supervisory Patent Examiner, Art Unit 2437

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: April 14, 2009.

/Aaron Emigh/
Aaron Emigh, Inventor

AMENDMENT A

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

Dear Sir:

This is in response to the Office Action mailed November 14, 2008. The following amendments and remarks are respectfully submitted.

AMENDMENTS TO THE SPECIFICATION

Please replace paragraph 0037 with the following rewritten paragraph:

[0037] Distributed update distribution is disclosed. In some embodiments, at least some users receive an update indirectly, e.g., from another user that received it previously, either directly from the original source or indirectly from a source that had itself earlier received it, again either directly or indirectly, and so on. Figures 3B-3D illustrate distributed update distribution as implemented according to some embodiments. In the example shown in Figures 3B-3D, it is assumed for expository purposes that each host that receives the update will serve as a redistribution node, each recipient has the ability to redistribute at the same rate as the original source, and there is continuous demand for the update from all sources. As shown in Figure 3B, at a time t1 a first direct recipient of the update D1 (332) downloads the update from the original source S[[1]] (330). As shown in Figure 3C, at a time t2 a second direct recipient D2 (334) downloads the update from the original source and an indirect recipient R11 (336) downloads the update from the first direct recipient D1 (332), which in this case acts as a redistribution node. As shown in Figure 3D, at a time t3 a third direct recipient D3 (338) downloads the update from original source S (330), a second indirect recipient R12 (340) downloads the update from the first direct recipient D1 (332), a third indirect recipient R21 (342) downloads the update from the second direct recipient D2, and a fourth indirect recipient R111 (344) downloads the update from first indirect recipient R11 (336). In this example, in the three download cycles shown in Figures 3B-3D on its own the original source would only have been able to download the update to the three direct recipients, but by using previous recipients to redistribute, in the example shown in Figures 3B-3D a total of seven recipients have been able to obtain the update. In a generalized case, under the assumptions used in this example in "n" download cycles/periods a total of 2n-1 recipients are able to obtain the update, whereas only "n" recipients, i.e., one per cycle, would otherwise have been able to obtain the update if it were only available directly from the original source. In an even more generalized case, under an assumption that each server may download roughly k copies in a time interval, for example where more than one download is provided by a server at a time, then in "n" download cycles (or periods) a total of roughly (k+1)n-1 recipients are able to obtain the update, where as only k*n recipients, i.e., k per cycle, would otherwise have been able to obtain the update if it were only available directly from the original source.

IN THE CLAIMS

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

Listing of Claims:

1. (currently amended) A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

2. (currently amended) A method as recited in claim 1, wherein detecting an insecure condition further includes at least one ~~or more~~ of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed~~, and querying the first host for a cleanliness assertion~~.

3. (canceled)

4. (original) A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.

5. (original) A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

6. (original) A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to a remediation host.

7. (original) A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.

8. (original) A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

9. (currently amended) A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and

a memory coupled to the processor and configured to provide instructions to the processor.

10. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion.

11. (canceled)

12. (currently amended) A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.

13. (original) A system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

14. (currently amended) A computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

15. (original) A method for processing requests from a quarantined host to communicate via a protected network, comprising:

receiving a service request sent by the quarantined host;

serving a quarantine notification page to the quarantined host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

16. (original) A method as recited in claim 15, further comprising, in the event the service request comprises a DNS query, proxying the service request to a DNS service if the host name that is the subject of the DNS query is associated with a remediation host.

17. (original) A method as recited in claim 15, wherein providing in response an IP address of a quarantine server includes providing a response with a short time to live.

18. (currently amended) A method for remedying an insecure condition in a host associated with a protected network, comprising:

detecting an open backdoor port on the host, wherein detecting the open backdoor port includes testing the host for an existence of at least one potential backdoor associated with a security vulnerability; and

using the open backdoor port to communicate with the host as required to remedy the insecure condition.

19. (canceled)

20. (canceled)

21. (new) A method as recited in claim 18, wherein the open backdoor port is associated with installation by at least one of a virus and a worm.

22. (new) A method as recited in claim 18, wherein the open backdoor port is associated with a buffer overrun exploit.

23. (new) A method as recited in claim 18, wherein communicating with the host as required to remedy the insecure condition includes exploiting the security vulnerability.

24. (new) A method as recited in claim 1, further comprising:

receiving a service request sent by the first host;

serving a quarantine notification page to the first host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

25. (new) A method as recited in claim 1, performed at an Internet service provider.

26. (new) A method as recited in claim 15, further comprising:

detecting an insecure condition on the quarantined host that has connected or is attempting to connect to a protected network;

quarantining the first host; and

permitting the first host to communicate with the remediation host.

27. (new) A method as recited in claim 15, performed at an Internet service provider.

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on April 14, 2009 between the Examiner, Supervisory Patent Examiner Emmanuel Moise, and the undersigned Applicant. The Office Action mailed on November 14, 2008 was discussed. The Examiner confirmed that she intended to reject claims 15-17 under 35 USC 102 as anticipated by Liang. The rejection of claims 1, 3 and 15 under 35 USC 102 as anticipated by Liang, and a potential amendment to claim 1 was discussed with the intent to place the claims in better condition for allowance or appeal. The Examiner stated that she believed the proposed amendment to claim 1 (as set forth in this Amendment) overcame the cited prior art, and that claim 15 overcomes the cited sections of the prior art as written.

Applicant wishes to thank the Examiner and SPE Moise for their time and attention in this case.

REMARKS

Claims 1, 2, 4-10, 12-18, and 21-24 are pending. Claims 3, 11, 19, and 20 have been canceled. Claims 1, 2, 9, 12, 14, and 18 have been amended. New claims 21-27 have been added. Support for the amendments and new claims can be found without limitation at paragraphs 29 and 50-55, and Figures 13-17, of the specification.

The Examiner has objected to the Specification on the grounds that the original source S1 (330) does not match the description in Figures 3B-3D. The Specification has been amended accordingly.

The Examiner has objected to claim 12 on the grounds that an omission was contained in the phrase "an operating is being performed." Claim 12 has been amended and is believed to be allowable.

The Examiner has rejected claim 19 under 35 USC 112 as being indefinite. Claim 19 has been canceled.

The Examiner has rejected claims 1-14 under 35 USC 102(e) as being anticipated by Liang (US 7,287,278). Although the Examiner did not explicitly reject claims 15-17, she conformed telephonically that her intent was to reject these claims under 35 USC 102(e) as anticipated by Liang. Applicant is therefore responding accordingly.

With respect to claims 1-14, Liang does not appear to teach or suggest "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness," nor "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network," as recited in amended independent claims 1 and 14, and similarly in amended independent claim 9.

Claims 1, 9, and 14 are therefore believed to be allowable.

Claims 2 and 4-8 depend from claim 1 and are believed to be allowable for the same reasons described above. Claim 3 has been canceled.

Claims 10, 12, and 13 depend from claim 9 and are believed to be allowable for the same reasons described above. Claim 11 has been canceled.

Applicant respectfully traverses the Examiner's rejection of claims 15-17 under 35 USC 102(e) as anticipated by Liang. Liang does not appear to teach or suggest "serving a quarantine notification page to the quarantined host if the service request comprises a web server request," nor "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host," as recited in independent claim 15.

Liang purports to teach that "in most cases, virus monitor 102 will direct the target client device…to an anti-virus installation server 138 (which may actually be the server 128) and *block any traffic to/from the target client device and all other addresses*..." (Liang, column 8, lines 41-46, emphasis added). Similarly, Liang purports to teach that "access to all addresses other than an anti-virus installation server 138 are *blocked* until a scan is made of the memory of the visitor client device 125" (Liang, column 9, lines 26-29, emphasis added). Furthermore, since Liang appears to describe software running on a client device, where Liang purports to teach that "a user interface can be displayed on the client device 116" (Liang, column 8, line 61), it appears to be discussing a user interface generated by software running on client device 116 rather than a web page served by a quarantine server, which is described, without limitation, at paragraph 54, and Figure 16, of the Specification. Applicant therefore believes that Liang not only does not teach or suggest the above-referenced elements of claim 15, but in fact teaches *away* from "providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host," and from "serving a quarantine notification page," as recited in independent claim 15. Claim 15 is therefore believed to be allowable.

Claims 16-17 depend from claim 15 and are believed to be allowable for the same reasons described above.

The Examiner has rejected claims 18 and 20 under 35 USC 102(e) as being anticipated by Hurst et al (US 6,996,845 B1), hereinafter referred to as Hurst. Applicant respectfully traverses the rejection. Hurst does not appear to teach or suggest "using the open backdoor port to communicate with the host as required to remedy the insecure condition," as recited in amended independent claim 18. The Examiner has cited Hurst, column 5, lines 36-39 and 44-49 as relevant to this limitation. However, the relevant lines recite "*port scanning (scanning a machine for open ports)* integrated with Web server discovery. By taking the information retrieved from a port scanner (port open on any given host) the Internet security analysis system 100 will attempt to ***determine*** whether that port is supporting HTTP or HTTPS" (Hurst, column 5, lines 36-39, emphasis added) and "When completed, the Internet security analysis system 100 will have a list of hosts that are currently hosting a web server and the port or ports on which the Web server is listening. The Internet security analysis system 100 will then take this list and pass it to the 'Webcrawl engine portion of the Internet security *analysis* system 100" (Hurst, column 5, lines 44-49, emphasis added). Hurst appears to be discussing information gathering and analysis, and not communicating with the host "as required to ***remedy*** the insecure condition," as recited in amended independent claim 18. Amended independent claim 18 is therefore believed to be allowable. Claim 20 has been canceled.

The Examiner has rejected claims 18-20 under 35 USC 102(e) as being anticipated by Currie et al (US 2003/0188194 A1), hereinafter referred to as Currie. Currie does not appear to teach or suggest "using the open backdoor port to communicate with the host as required to remedy the insecure condition," as recited in amended independent claim 18. The Examiner has cited Currie, page 3, paragraph 40 as relevant to this limitation. However, the cited paragraph recites "Scanning engine 302 can include any conventionally known remote security scanner or equivalent thereof, such as the open source Nessus engine (details available from www.nessus.org), that remotely obtains and ***produces information about*** open ports, available services, network protocols, security exposures and vulnerabilities existing on a server or other device that is available over a network. Accordingly, scanning engine 302 periodically checks the web servers and/or network devices of service 102 to ***discover*** website component configuration and vulnerabilities. Scanning engine 302 initially scans the open ports of devices registered in customer information database 304. In one example implementation such as the Nessus open source engine, the scanning process *produces a set of XML files containing all information gathered during the scan*. These files are parsed by scanning engine 302 and stored

in database 304, the records of which are associated with the customer account number and therefore the customer's registration information" (emphasis added). Currie appears to be discussing ways to *produce information about* ports and *discovering* vulnerabilities, and not communicating with the host "as required to *remedy* the insecure condition," as recited in amended independent claim 18. Amended independent claim 18 is therefore believed to be allowable. Claims 19 and 20 have been canceled.

New claims 21-23 depend from claim 18 and are believed to be allowable for the same reasons described above.

New claims 24 and 25 depend from claim 1 and are believed to be allowable for the same reasons described above.

New claims 26 and 27 depend from claim 15 and are believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: April 14, 2009

/Aaron Emigh/
Aaron Emigh, Inventor
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237003
Filing Date:	27-Sep-2005
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-034

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	3	26	78
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	2252	1	245	245
Miscellaneous:				
			Total in USD ($)	**323**

Electronic Acknowledgement Receipt

EFS ID:	5154874
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	14-APR-2009
Filing Date:	27-SEP-2005
Time Stamp:	22:47:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$323
RAM confirmation Number	5297
Deposit Account	504831
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		PB-034-amendment-a.pdf	123719 8844276a1475b66a5041b9899a19c8c35fc2267d	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Claims	3	6
Applicant summary of interview with examiner	7	7
Applicant Arguments/Remarks Made in an Amendment	8	11

Warnings:

Information:

2	Fee Worksheet (PTO-06)	fee-info.pdf	31547 0c53800daedae457728530b1c4aa42239afd1e766	no	2

Warnings:

Information:

Total Files Size (in bytes):	155266

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/237,003	09/27/2005	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	04/14/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 20	= 3	X $26 =	78	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 5	Minus	***5	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	78	OR	TOTAL ADD'L FEE	

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/TARA J. WITCHER/

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.

PTOL-413A (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office : U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

ATTORNEY DOCKET NO. PB-034

Application No.: 11/237,003 First Named Applicant: Roskind
Examiner: Sims, Jing F. Art Unit: 4148 Status of Application: Pending

Tentative Participants:

(1) Aaron Emigh (2) _____

(3) _____ (4) _____

☐ ☒

Proposed Date of Interview: April 14, 2009 Proposed Time: 1:00 (AM/PM)

Type of Interview Requested:

(1) ☒ Telephonic (2) ☐ Personal (3) ☐ Video Conference

Exhibit To Be Shown or Demonstrated: ☐ YES ☒ NO

If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rejection	3	Liang	[ ]	[ ]	[ ]
(2) Rejection	15	Liang	[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Arguments to be Presented:

Discuss "trusted computing base" (claim 3) and how best to claim in a manner that overcomes the prior art.

Discuss claim 15 since Liang does not appear to teach/suggest the limitations as understood by Applicant.

Guidance on how best to move forward toward allowance.

An interview was conducted on the above-identified application on _____.

NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

/Aaron T. Emigh/

Applicant/Applicant's Representative Signature

Aaron T. Emigh, inventor

Typed/Printed Name of Applicant or Representative

Registration Number, if applicable

Examiner/SPE Signature

This collection of information is required by 37 CFR 1.133. 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 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Electronic Acknowledgement Receipt

EFS ID:	5144238
Application Number:	11237003
International Application Number:	
Confirmation Number:	5151
Title of Invention:	Contagion isolation and inoculation
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-034
Receipt Date:	13-APR-2009
Filing Date:	27-SEP-2005
Time Stamp:	16:50:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	First Action Interview - Schedule Interview request	PB-034-interview-request.pdf	26906 e61d4e307cc3ba76995466828ceacfe61a0e345b	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	26906

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/237,003	09/27/2005	James A. Roskind	RAD2P001

CONFIRMATION NO. 5151

POA ACCEPTANCE LETTER

85853
Aaron Emigh
762 Judith Court
Incline Village, NV 89451

OC000000034785129

Date Mailed: 03/03/2009

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/23/2009.

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.

/hgray/

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: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/237,003	09/27/2005	James A. Roskind	RAD2P001

CONFIRMATION NO. 5151

POWER OF ATTORNEY NOTICE

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

OC000000034785068

Date Mailed: 03/03/2009

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/23/2009.

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

/hgray/

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

OIPE
FEB 23 2009
PATENT & TRADEMARK OFFICE

JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.	RAD2P001

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in a prepaid envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

February 18, 2009.

Inventor

REVOCATION OF POWER OF ATTORNEY

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

We hereby revoke all previous powers of attorney given in the above-identified patent application under 37 CFR §1.36.

We are the applicants and inventors of the above-identified patent application.

Signature	Name	Date
	James A. Roskind	January 26, 2009
	Aaron T. Emigh	January 26, 2009

OIPE
FEB 23 2009
PATENT & TRADEMARK OFFICE

JFW

PTO/SB/122 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Application

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

Application Number	11/237,003
Filing Date	9/27/2005
First Named Inventor	Roskind
Art Unit	4148
Examiner Name	Sims, Jing F.
Attorney Docket Number	RAD2P001

Please change the Correspondence Address for the above-identified patent application to:

☑ The address associated with Customer Number: 85853

OR

☐ Firm or Individual Name

Address

City | State | Zip

Country

Telephone | Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

☑ Applicant/Inventor

☐ Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☐ Attorney or agent of record. Registration Number _____.

☐ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number _____.

Signature

Typed or Printed Name: Aaron T. Emigh

Date: January 26, 2009 | Telephone: 415-297-1305

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

☑ *Total of 2 forms are submitted.

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

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

OIPE
FEB 23 2009
PATENT & TRADEMARK OFFICE

PTO/SB/122 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Application

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

Application Number	11/237,003
Filing Date	9/27/2005
First Named Inventor	Roskind
Art Unit	4148
Examiner Name	Sims, Jing F.
Attorney Docket Number	RAD2P001

Please change the Correspondence Address for the above-identified patent application to:

☑ The address associated with Customer Number: 85853

OR

☐ Firm or Individual Name

Address

City | State | Zip

Country

Telephone | Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

☑ Applicant/Inventor

☐ Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☐ Attorney or agent of record. Registration Number _____.

☐ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number_____.

Signature

Typed or Printed Name James A. Roskind

Date January 26, 2009 | Telephone 650-274-9617

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

☑ *Total of 2 forms are submitted.

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	RAD2P001	5151

21912 7590 11/14/2008

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
SIMS, JING F	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

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

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	4148	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2005*.

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

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

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

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☒ Claim(s) *12* is/are objected to.

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

Application Papers

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

10)☒ The drawing(s) filed on *27 September 2005 and 28 October 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 11237003 filed on 09/27/2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Priority

3. As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on 09/27/2004 (US Provisional Application 60613909).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

4. The applicant's drawings submitted are acceptable for examination purposes.

Specification

5. The disclosure is objected to because of the following informalities:

The original source S1 (330) does not match the description in Fig. 3B-3D. The Figures use S to represent the original source.

Appropriate correction is required.

Claim Objections

6. Claim 12 is objected to because of the following informalities: on page 36, line 2-3, the claim description of “after installation of an operating is being performed” appears to be after installation of an operating system is being performed. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 19 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 19, the limitation "communicate cannot be established with the host using a primary communication method” is indefinite. The claim does not particularly point out or distinctly the subject matter in the limitation(s). Examiner is not able to conduct a search based on this claim language; therefore, examiner does not examine the limitation on the merit.

Claim Rejections - 35 USC § 102

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

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

10. **Claims 1-14** are rejected under 35 U.S.C. 102(e) as being anticipated by Liang. (US 7287278 B2).

As per claim 1, Liang discloses "a method for protecting a network, comprising: detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network) "quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems) "and permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

As per claim 2, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes one or more of the following: scanning for a

vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 3, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes querying the first host for a cleanliness assertion, including by: contacting a trusted computing base within the first host; and requesting an authenticated infestation scan by trusted software" (col. 8, line 49-64, upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files); and in line 16-18, Liang teaches the OPP files is used to apply appropriate virus policies to scan for viruses).

As per claim 4, Liang discloses “a method as recited in claim 1, wherein detecting an insecure condition includes 20 determining that the first host should be quarantined until an update to an operating system has been installed” (col. 8 line 55-64, if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 5, Liang discloses “a method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system” (col. 17, line 47-55, identifying a new client device to e added to the network. Identification includes identifying the type of system, resident operating system etc. In col. 18, line 4-7, if the new client has been determined that proper anti-virus policies and protocols are not in place, then all access to all addresses except to that of an anti-virus software installation server are blocked. Liang teaches the client need to meet certain safety policies and protocols to access the network. The initial startup after installation of the operating system is the configuration of the system, therefore, it is the policies and protocols).

As per claim 6, Liang discloses “a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to a remediation host” (col. 15, line 47-57, the security module has determined that a particular those data packets found to be virus-free are sent back to the network traffic flow).

As per claim 7, Liang discloses “a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host” (col. 15, line 47-57, the security module has determined that a particular data packets deemed more likely to be affected are passed directly to the file scan module. A data packet is always has its purpose to request service from the destination network and it is usually not address to a remediation host).

As per claim 8, Liang discloses “a method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition” (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 9, Liang discloses “a system for protecting a network, comprising: a processor configured to: detect an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor monitors activities of network, detecting abnormal events from other computers that on the network. Liang also describes virus monitors can be a stand alone server computer in col. 7, line 15-21) “quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network” (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems) “and permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition” (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak) “and a memory coupled to the processor and configured to provide instructions to the processor” (col. 7, line 15-21, virus monitors can be a stand alone server computer. Every stand alone computer includes memory and processor).

As per claim 10, Liang discloses “a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data” (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) “checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion” (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 11, Liang discloses “a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by: contacting a trusted computing base within the first host; and requesting an authenticated infestation scan by trusted software” (col. 8, line 49-64, upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files); and in line 16-18, Liang teaches the OPP files is used to apply appropriate virus policies to scan for viruses).

As per claim 12, Liang discloses “a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating is being performed” (col. 7, line 25-36, the controller includes a rules engine used to store and source of detection rules for detecting computer viruses and an outbreak prevention policy distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak. Liang also discloses the policies, protocols and procedures can be periodically updated. Checking initial startup after installation of an OS is regular procedure to perform for securing of a computer, therefore the rules, polices, or procedures that Liang described include that checking initial startup after installation of an OS).

As per claim 13, Liang discloses “a system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition” (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 14, Liang discloses “a computer program product for protecting a network, the computer program product being embodied in a computer readable medium and comprising computer instructions for” (col. 3, line 44-45, and line 59-67, a computer program project for monitoring a network for computer viruses) “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network” (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network) “quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network” (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems) “and permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition” (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

As per claim 15, Liang discloses “a method for processing requests from a quarantined host to communicate via a protected network, comprising: receiving a service request sent by the quarantined host; serving a quarantine notification page to the quarantined host if the service request comprises a web server request” (col. 17, line 64-67, and col. 18, 1-16, if the new client device has been determined that the proper anti-virus policies and protocols are not in place, then all access to all address are blocked. Since the new device has been block it must be a quarantine notification to the host/device); “and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host” (col. 18, line 1-16, all access to all addresses except to that of an anti-virus software installation server are blocked).

As per claim 16, “a method as recited in claim 15, further comprising, in the event the service request comprises a DNS query, proxying the service request to a DNS service if the host name that is the subject of the DNS query is associated with a remediation host” (col. 18, line 1-16, all access to all addresses except to that of an anti-virus software installation server are blocked. An anti-virus software installation server is considered as a remediation host).

As per claim 17, “a method as recited in claim 15, wherein providing in response an IP address of quarantine serve includes providing a response with a short time to live” (col. 18, line 7-16, once access to the anti-virus software installation server is granted, then a determination is made whether or not the appropriate anti-virus software is to be downloaded to the new device. If it is determined not to be downloaded, then the process ends without the new client device being connected to the network. The process shows aiding a return to normal routing of traffic once the computer is no longer under quarantine).

11. **Claims 18 and 20** are rejected under 35 U.S.C. 102(e) as being anticipated by Hurst et al. (US 6996845 B1) (hereinafter Hurst).

As per claim 18, Hurst discloses “a method for remedying an insecure condition in a host associated with a protected network, comprising: detecting an open backdoor port on the host” (col. 5, line 33-37, Internet security analysis system is port scanning (scanning a machine for open ports)) “and using the open backdoor port to communicate with the host as required to remedy the insecure condition” (in the instant application using the open backdoor port communicate with the host in one instance is to causes a success code to be returned by a command. Hurst teaches that by taking the information retrieved from a port scanner (port open on any given host) the Internet security analysis system will attempt to determine some conclusion in col. 5, line 36-39. Col. 5, line 44-49, Internet security analysis system will take the list of hosts that the port or ports is listening and it to the other potion of the Internet security analysis system. This allows an ability to look for web vulnerabilities).

As per claim 19, “a method as recited in claim 18, further comprising determining that communication cannot be established with the host using a primary communication method” (col. 3, paragraph 41).

As per claim 20, “a method as recited in claim 18, wherein detecting an open backdoor port on the host includes scanning the host for any open backdoor port” (col. 5, line 33-37, Internet security analysis system is port scanning (scanning a machine for open ports)).

12. **Claims 18-20** are rejected under 35 U.S.C. 102(e) as being anticipated by Currie et al. (US 2003/0188194 A1) (hereinafter Currie).

As per claim 18, Currie discloses “a method for remedying an insecure condition in a host associated with a protected network, comprising: detecting an open backdoor port on the host” (page 3, paragraph 40, scanning engine remotely obtains about open ports information on a server or device over a network) “and using the open backdoor port to communicate with the host as required to remedy the insecure condition” (page 3, paragraph 40, scanning engine scans the open ports of devices, then the scanning process produces a set of XML files containing all information gathered during the scan. The records of which are associated with the customer account number and therefore the customer's registration information. It clearly shows the scanning engine communicates with the host by its open backdoor port to gather the registration information).

As per claim 19, Currie discloses "a method as recited in claim 18, further comprising determining that communication cannot be established with the host using a primary communication method" (page 3, paragraph 41, the stored information includes what sockets are open on the scanned device, what generic services should be running on those ports, and what services are actually running on the open ports. This indicates the services should be running on the ports but not actually running is due to the primary communication uses on the port).

As per claim 20, Currie discloses "a method as recited in claim 18, wherein detecting an open backdoor port on the host includes scanning the host for any open backdoor port" (page 3, paragraph 40, scanning engine remotely obtains about open ports information on a server or device over a network).

Conclusion

13. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See **MPEP 707.05(c)**.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-4:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (572)272-3689. 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.

November 6th, 2008 Jing Sims

/J.S./
Examiner, Art Unit 4148

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148

Notice of References Cited	Application/Control No. 11/237,003	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner JING SIMS	Art Unit 4148	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,287,278	10-2007	Liang, Yung Chang	726/22
*	B	US-6,996,845	02-2006	Hurst et al.	726/25
*	C	US-2003/0188194	10-2003	Currie et al.	713/201
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	Art Unit
	JING SIMS	4148

SEARCHED			
Class	Subclass	Date	Examiner
726	22,23	11/3/2008	JS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in EAST		JS
Text Searcg (see EAST notes)		JS

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237003	ROSKIND ET AL.
	Examiner	**Art Unit**
	JING SIMS	4148

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

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	42	quarant$3 near3 (server or host or computer) same communicat$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:49
L3	40	quarant$3 near3 (server or host or computer) same virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:53
L4	527	quarant$3 same virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:55
L5	400	quarant$3 same virus and computer	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:57
L6	399	quarant$3 same virus and computer and system	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:57
L7	225	quarant$3 same virus and computer and system and IP	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 09:58
L8	31	quarant$3 same virus and remediation	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:00
L9	77	quarant$3 same (computer near3 virus)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:02
L10	252	(quarant$3 or isolat3) with (computer or server) and virus	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 10:35
L14	1345	726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:44
L15	1345	726/22.ccls. and ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:45
L16	11	726/22.ccls. and (re $1direct or allow$ or forbid$ or isolat$ or limit$) near (compromise$ or quarantine$)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:46

L17	3	726/22.ccls. and (re $1direct or allow$ or forbid$ or isolat$ or limit$) near (quarantine$)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:51
L18	9624	DNS same IP	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
L19	646	DNS same IP same redirect$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
L20	658	DNS same IP same re $direct$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 12:59
L21	341	DNS same IP same re $direct$3 and @ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:00
L22	686	726/22.ccls. and @ay<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:17
L23	32	726/22.ccls. and @ay<="2003" and quaranti$2	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 13:18
L24	0	scan with open near3 back$1door	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:38
L25	0	scan$4 with open near3 back$1door	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:38
L26	217	scan$4 with open near3 (back$1door or port)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:39
L27	23	scan$4 with open near3 (back$1door or port) and 726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:40
L28	0	(detect$3 near3 (open near$3 port))and scan $4 with open near3 (back$1door or port) and 726/22.ccls.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 14:55
L29	0	dns with (short$time to live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
L30	0	dns same (short$time to live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10
L31	13	(short$time near3 live)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:10

L32	0	(short$time near3 live) and DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:11
L33	933	(726/23).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2008/11/07 18:31
L34	933	726/23.CCLS.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
L35	0	726/23.CCLS. AND @AD<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
L36	536	726/23.CCLS. AND @AY<="2003"	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/07 18:32
S1	0	11/237003.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 08:58
S2	0	60/613909.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 09:03
S3	0	11/237004.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:49
S4	1	11/237119.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:50
S5	0	11/237199.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 16:50
S6	15	((JAMES) near2 (ROSKIND)).INV.	USPAT	ADJ	ON	2008/11/03 16:51
S7	1	((AARON) near2 (EMIGH)).INV.	USPAT	ADJ	ON	2008/11/03 16:56
S8	120335	network near3 access	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:14
S9	73	detect$3 same (redirect$3 or forward $3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:16
S10	5527	protect near4 network	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/03 17:17
S11	80	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 10:21

S12	0	"9478944".pn.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:44
S13	0	"9478944".pn.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:44
S14	0	"10756682".app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:45
S15	1	09/478944.app.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:47
S16	7	"478944".ap.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 16:54
S17	80	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:11
S18	1	S16 and S17	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:11
S19	0	METHOD AND SYSTEM FOR PROTECTING A COMPUTER USING A REMOTE E-MAIL SCANNING DEVICE.ti.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:18
S20	1	REMOTE E-MAIL SCANNING DEVICE.ti.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:18
S21	833	kim-do-$.in.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:20
S22	2	kim-do-k.in.	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/04 17:20
S23	25	(detect$3 or scan$3) same (redirect$3 or forward$3) same quarant$3 and (protect $3 near2 network)	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/05 09:12
S24	3	quarant$3 same remediat$3 same DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/06 16:32
S25	35	quarant$3 same DNS	US-PGPUB; USPAT; IBM_TDB	ADJ	ON	2008/11/06 16:40

11/7/2008 6:48:46 PM
C:\Documents and Settings\jsims2\My Documents\EAST\Workspaces\11237003.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 5151

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/237,003	09/27/2005	707	4148	RAD2P001

APPLICANTS

James A. Roskind, Redwood City, CA;
Aaron T. Emigh, Incline Village, NV;

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

This appln claims benefit of 60/613,909 09/27/2004

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

10/14/2005

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /JING F SIMS/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	25	20	5

ADDRESS

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014
UNITED STATES

TITLE

Contagion isolation and inoculation

FILING FEE RECEIVED		
700	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

1 fw

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/237,003	09/27/2005	James A. Roskind	RAD2P001

OIPE IAP75 OCT 28 2005 PATENT & TRADEMARK OFFICE

CONFIRMATION NO. 5151

FORMALITIES LETTER

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

Date Mailed: 10/14/2005

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 made on paper that has a white background (see 37 CFR 1.84 (e)). For example, drawings on graph paper, lined paper, or paper that has a non-white background are not acceptable. See Figure(s) 2b, 3b-d, 4b-c, 10b, 19b.

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

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

E. J

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382

PART 2 - COPY TO BE RETURNED WITH RESPONSE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al.	Examiner:	Not Assigned
Application No.:	11/237,003	Art Unit:	2161
Filed:	September 27, 2005	Docket No.:	RAD2P001
Title:	CONTAGION ISOLATION AND INOCULATION		

OIPE
IAP75
OCT 28 2005
PATENT & TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in a prepaid envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Oct. 26, 2005.

Veronica Pula

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

MAIL STOP MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a Response to Notice to File Corrected Application Papers mailed **October 14, 2005.**

Application Elements:

☐ Declaration

☐ Newly executed (original or copy)

☐ Copy from a prior application (37 CFR 1.63(d) for a continuation or divisional). The entire disclosure of the prior application from which a copy of the declaration is herein supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

☐ Deletion of inventors Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

Accompanying Application Parts:

☐ Information Disclosure Statement with Form PTO-1449 ☐ Copies of IDS Citations

☐ Preliminary Amendment (*New claims numbered after highest original claim in prior application.*)

☒ Return Receipt Postcard

☒ Copy of Notice to File Corrected Application Papers

☒ Other: Six (6) Sheets of Corrected Application Papers

Amendments

☐ Cancel in this application original claims _____ of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

					Small Entity			Large Entity	
					Rate	Fee		Rate	Fee
Filing Fees					x $150 = $		OR	x $300 = $	
Search Fees					x $250 = $		OR	x $500 = $	
Examination Fees					x $100 = $		OR	x $200 = $	
CLAIMS	Filed.		Extra						
Total		Less 20	-0-		x $25 = $		OR	x $50 = $	
Independent		Less 3	-0-		x $100 = $		OR	x $200 = $	
Multiple Dependent Claims			-0-		x $180 = $		OR	x $360 = $	
Declaration and Surcharge Fee					X $65 = $		OR	X $130 = $	
					TOTAL FILING FEE $			TOTAL FILING FEE $	0

☐ Applicants petition for an extension of time to respond under 37 CFR § 1.136(a) as follows:

	SMALL ENTITY			LARGE ENTITY	
	Rate	Add'l Fee		Rate	Add'l Fee
☐ Extension for Response within FIRST month	x $60 = $		OR	x $120 = $	
☐ Extension for Response within SECOND month	x $225 = $		OR	x $450 = $	
☐ Extension for Response within THIRD month	x $510 = $		OR	x $1020 = $	
☐ Extension for Response within FOURTH month	x $795 = $		OR	x $1590 = $	
☐ Extension for Response within FIFTH month	x $1080 = $		OR	x $2160 = $	

☐ Check No. _____ for $_____ is enclosed.

General Authorizations

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed to Deposit Account No. 50-0685 (Order No. RAD2P001).

☒ The Commissioner is given general authorization to charge any fees or to credit any overpayment during the pendency of this application to Deposit Account No. 50-0685 (Order No. RAD2P001).

☒ Please send correspondence to the following address:

Customer No. 21912
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd.
Suite 200
Cupertino, CA 95014

Date: 10/24/05

William J. James
Reg. No. 40,661

1 fw

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/237,003	09/27/2005	James A. Roskind	RAD2P001

OIPE IAP75 OCT 28 2005 PATENT & TRADEMARK OFFICE

CONFIRMATION NO. 5151

FORMALITIES LETTER

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

Date Mailed: 10/14/2005

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 made on paper that has a white background (see 37 CFR 1.84 (e)). For example, drawings on graph paper, lined paper, or paper that has a non-white background are not acceptable. See Figure(s) 2b, 3b-d, 4b-c, 10b, 19b.

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

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

E. J

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382

PART 2 - COPY TO BE RETURNED WITH RESPONSE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al.	Examiner:	Not Assigned
Application No.:	11/237,003	Art Unit:	2161
Filed:	September 27, 2005	Docket No.:	RAD2P001
Title:	CONTAGION ISOLATION AND INOCULATION		

OIPE
IAP75
OCT 28 2005
PATENT & TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in a prepaid envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Oct. 26, 2005.

Veronica Pula

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

MAIL STOP MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a Response to Notice to File Corrected Application Papers mailed **October 14, 2005.**

Application Elements:

☐ Declaration

☐ Newly executed (original or copy)

☐ Copy from a prior application (37 CFR 1.63(d) for a continuation or divisional). The entire disclosure of the prior application from which a copy of the declaration is herein supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

☐ Deletion of inventors Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

Accompanying Application Parts:

☐ Information Disclosure Statement with Form PTO-1449 ☐ Copies of IDS Citations

☐ Preliminary Amendment (*New claims numbered after highest original claim in prior application.*)

☒ Return Receipt Postcard

☒ Copy of Notice to File Corrected Application Papers

☒ Other: Six (6) Sheets of Corrected Application Papers

Amendments

☐ Cancel in this application original claims _____ of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

					Small Entity			Large Entity	
					Rate	Fee		Rate	Fee
Filing Fees					x $150 = $		OR	x $300 = $	
Search Fees					x $250 = $		OR	x $500 = $	
Examination Fees					x $100 = $		OR	x $200 = $	
CLAIMS	Filed.		Extra						
Total		Less 20	-0-		x $25 = $		OR	x $50 = $	
Independent		Less 3	-0-		x $100 = $		OR	x $200 = $	
Multiple Dependent Claims			-0-		x $180 = $		OR	x $360 = $	
Declaration and Surcharge Fee					X $65 = $		OR	X $130 = $	
					TOTAL FILING FEE $			TOTAL FILING FEE $	0

☐ Applicants petition for an extension of time to respond under 37 CFR § 1.136(a) as follows:

	SMALL ENTITY			LARGE ENTITY	
	Rate	Add'l Fee		Rate	Add'l Fee
☐ Extension for Response within FIRST month	x $60 = $		OR	x $120 = $	
☐ Extension for Response within SECOND month	x $225 = $		OR	x $450 = $	
☐ Extension for Response within THIRD month	x $510 = $		OR	x $1020 = $	
☐ Extension for Response within FOURTH month	x $795 = $		OR	x $1590 = $	
☐ Extension for Response within FIFTH month	x $1080 = $		OR	x $2160 = $	

☐ Check No. _____ for $_____ is enclosed.

General Authorizations

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed to Deposit Account No. 50-0685 (Order No. RAD2P001).

☒ The Commissioner is given general authorization to charge any fees or to credit any overpayment during the pendency of this application to Deposit Account No. 50-0685 (Order No. RAD2P001).

☒ Please send correspondence to the following address:

Customer No. 21912
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd.
Suite 200
Cupertino, CA 95014

Date: 10/24/05

William J. James
Reg. No. 40,661

OIPE IAP75
OCT 28 2005
PATENT & TRADEMARK OFFICE

STAEDTLER® No. 937 811E
Engineer's Computation Pad

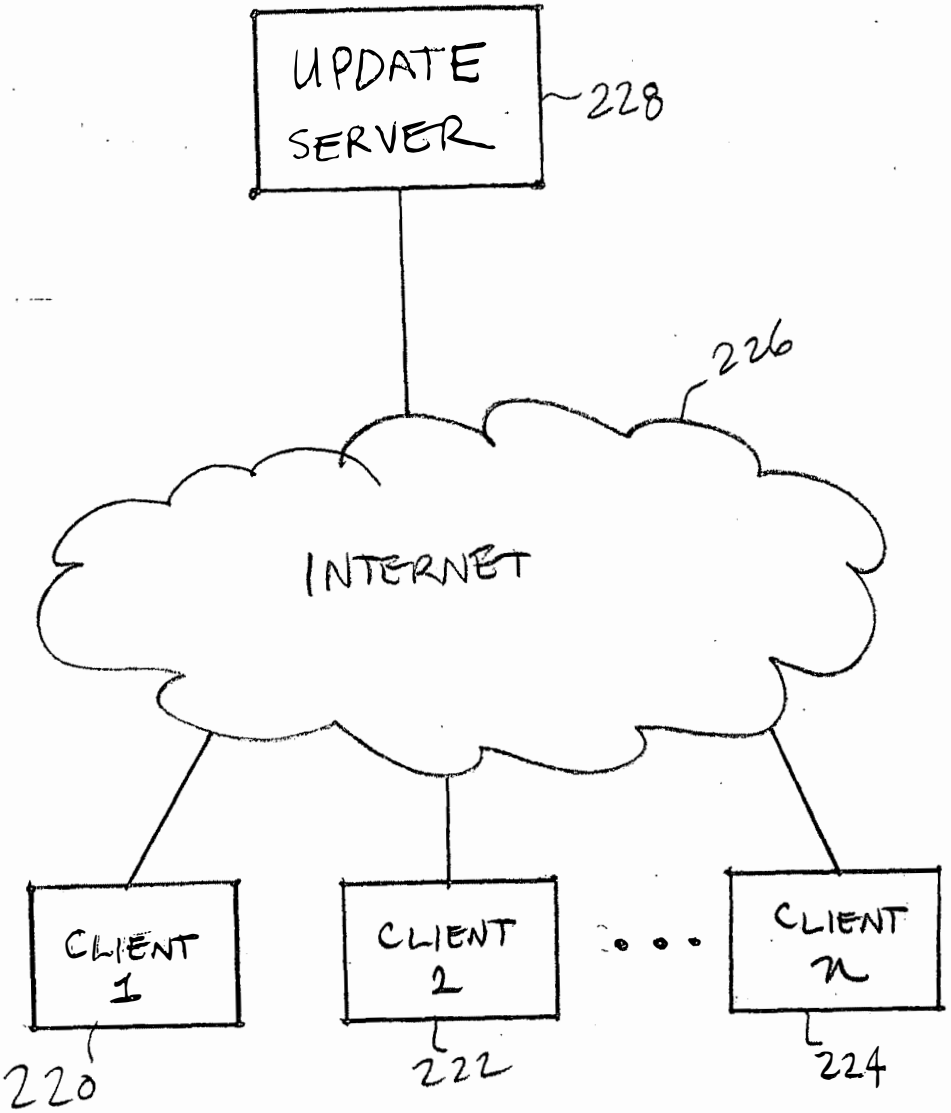


FIG. 2B

STAEDTLER® No. 937 811E
Engineer's Computation Pad

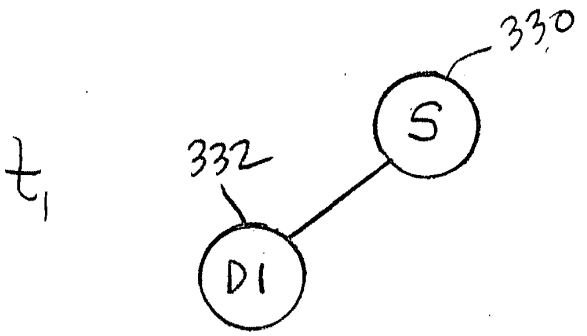


FIG. 3B

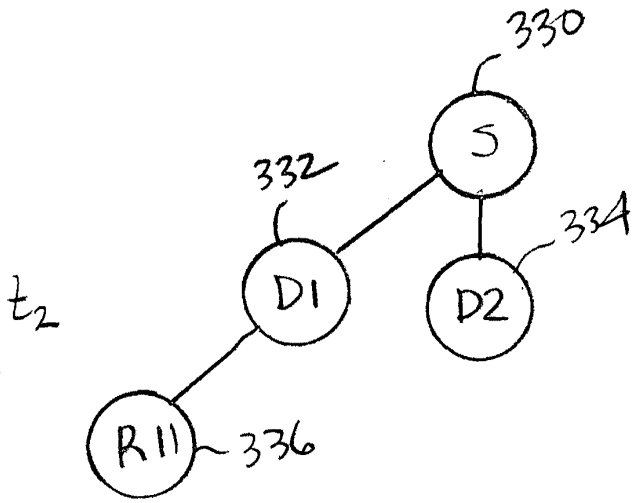


FIG. 3C

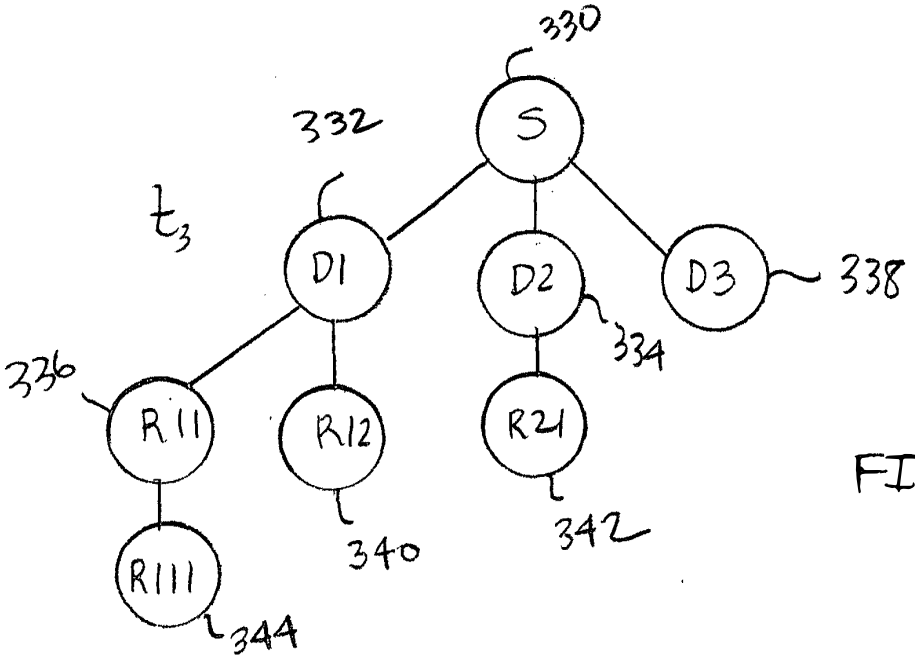


FIG. 3D

STAEDTLER® No. 937 811E
Engineer's Computation Pad

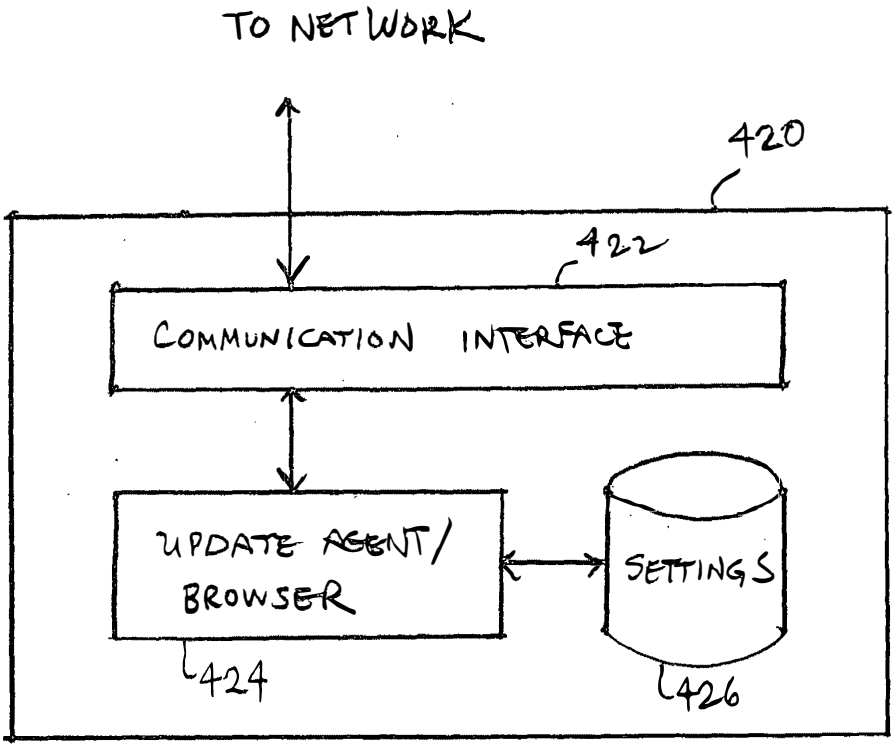


FIG. 4B

STAEDTLER® No. 937 811E
Engineer's Computation Pad

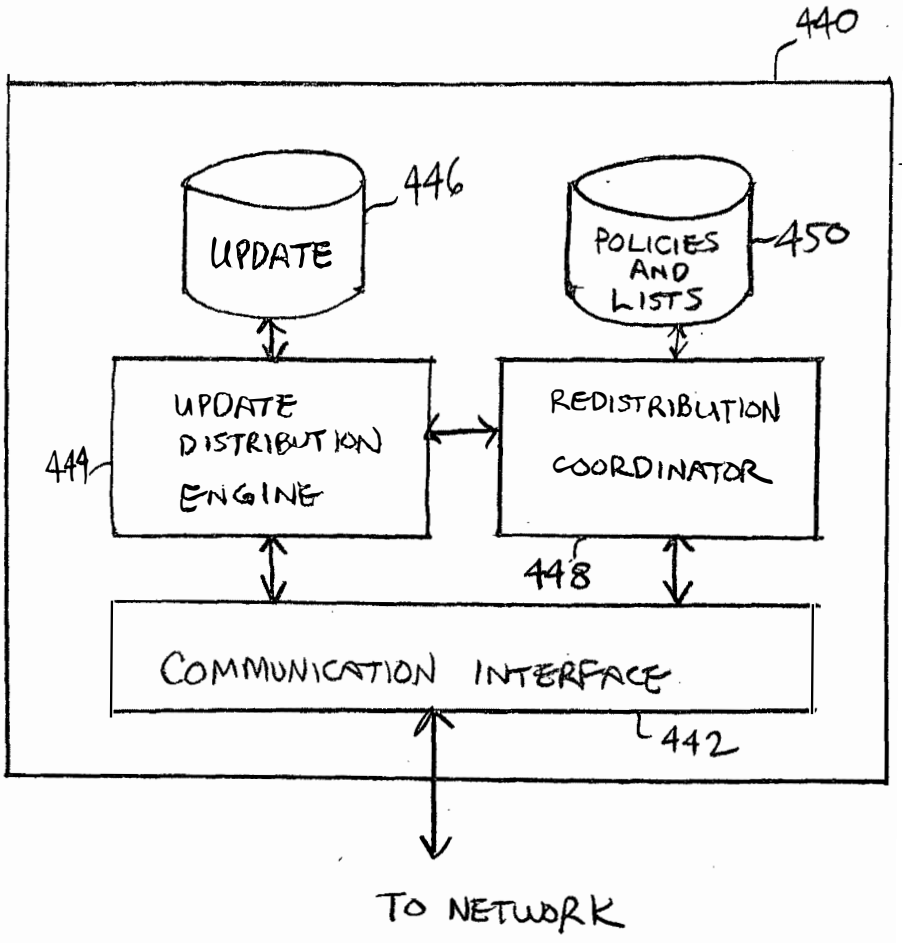


FIG. 4C

STAEDTLER® No. 937 811E Engineer's Computation Pad

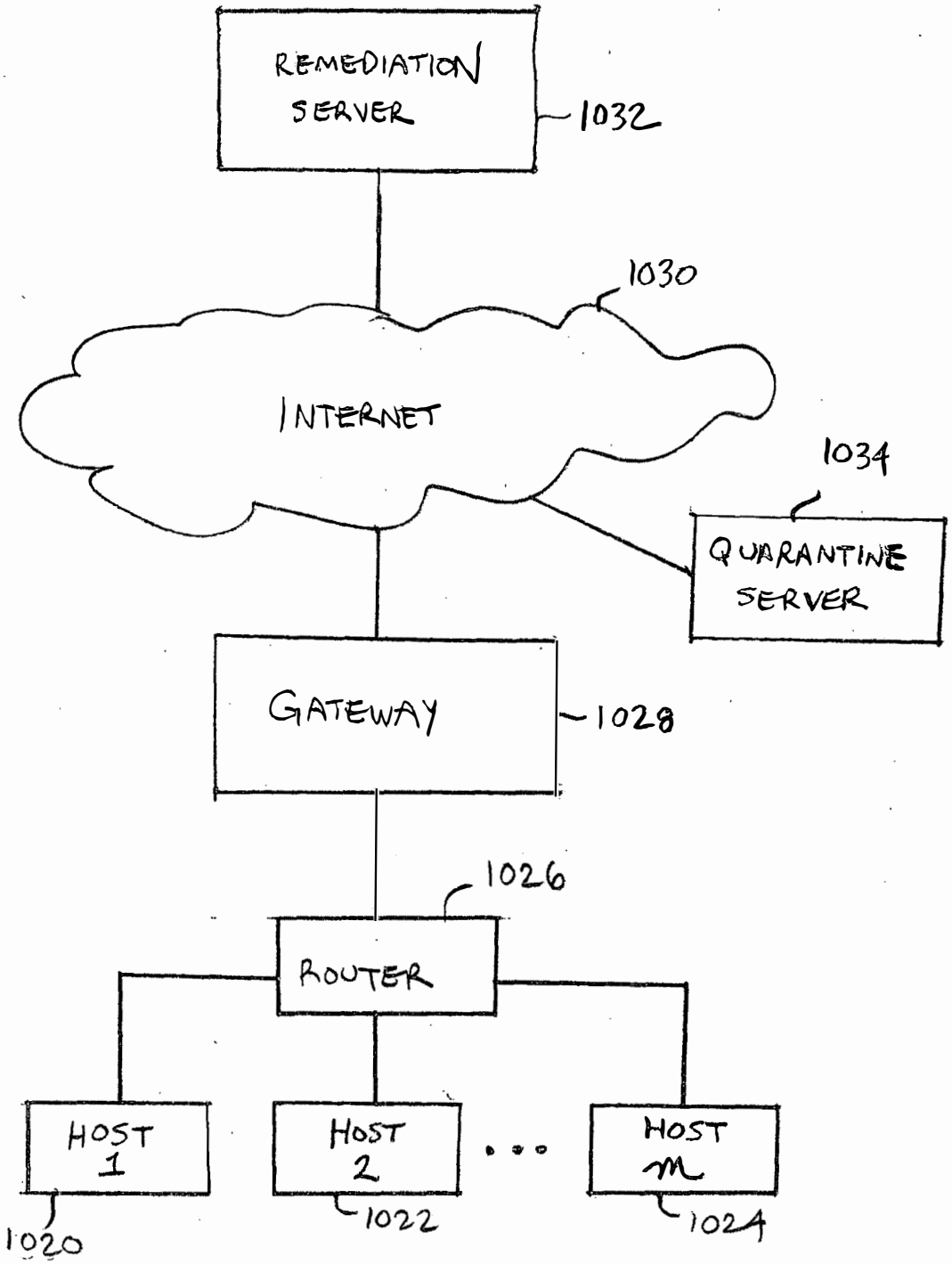


FIG. 10B

STAEDTLER® No. 937 811E
Engineer's Computation Pad

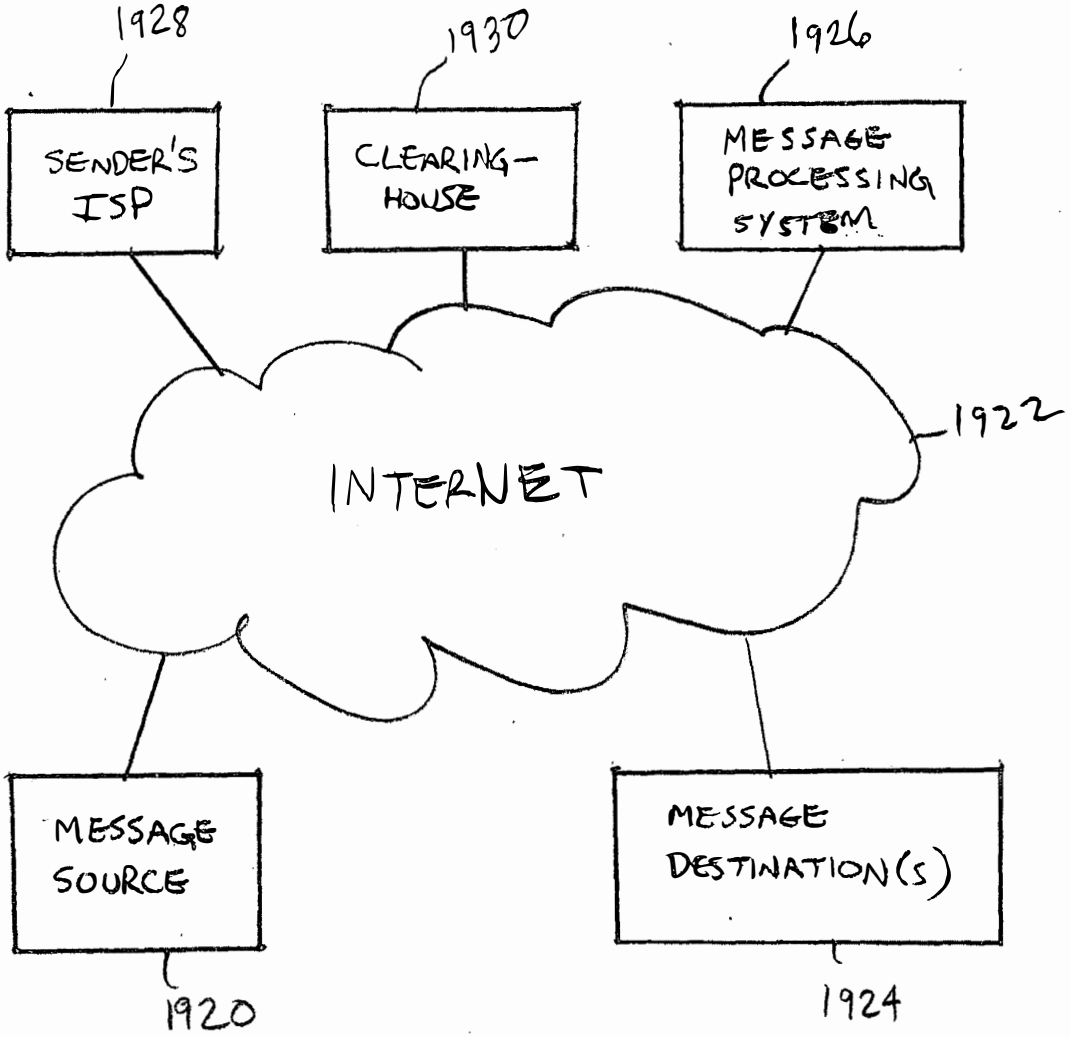


FIG. 19B

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/237,003	09/27/2005	James A. Roskind	RAD2P001

CONFIRMATION NO. 5151

FORMALITIES LETTER

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

Date Mailed: 10/14/2005

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 made on paper that has a white background (see 37 CFR 1.84 (e)). For example, drawings on graph paper, lined paper, or paper that has a non-white background are not acceptable. See Figure(s) 2b, 3b-d, 4b-c, 10b, 19b.

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

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

ET

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382

PART 3 - OFFICE COPY

16638 U.S. PTO
092705

UTILITY PATENT APPLICATION TRANSMITTAL

Under Small Entity Status

(New Nonprovisional Applications Under 37 CFR § 1.53(b))

Attorney Docket No. RAD2P001

112959 U.S. PTO
11/237003
092705

TO THE COMMISSIONER FOR PATENTS:

Transmitted herewith is the patent application of ( ) application identifier or (X) first named inventor, James A. Roskind, entitled CONTAGION ISOLATION AND INOCULATION, for a(n):

(X) Original Patent Application.

( ) Continuing Application (prior application not abandoned):
( ) Continuation ( ) Divisional ( ) Continuation-in-part (CIP)
of prior Application No. _____, filed _____.

( ) Please add after the title of the application "This is a
( ) Continuation ( ) Divisional ( ) Continuation-in-part (CIP)
of Application No. _____, filed _____, which is hereby incorporated by reference."

(X) This application claims the benefit of U.S. Provisional Application No. 60/613,909 , filed September 27, 2004.

Enclosed are:
(X) Specification; 38 Total Pages. (X) Drawing(s); 25 Total Sheets.
(X) Oath or Declaration:
(X) A Newly Executed Combined Declaration and Power of Attorney:
(X) Signed. ( ) Unsigned. ( ) Partially Signed.
( ) A Copy from a Prior Application for Continuation/Divisional (37 CFR § 1.63(d)).
( ) Signed Statement Deleting Inventor(s) Named in the Prior Application. (37 CFR § 163(d)(2)).
( ) Power of Attorney. (X) Return Receipt Postcard.
( ) Associate Power of Attorney. (X) A Check in the amount of $700.00 for the Filing Fee.
( ) Preliminary Amendment. ( ) Information Disclosure Statement and Form PTO-1449.
( ) A Duplicate Copy of this Form for Processing Fee Against Deposit Account.
( ) A Certified Copy of Priority Documents (if foreign priority is claimed).
( ) Assignment and Assignment Recordation Cover Sheet
(X) Applicant(s) hereby claim Status as a Small Entity.
( ) Statement(s) of Status as a Small Entity Filed in Prior Application, Status Still Proper and Desired.
(X) Non Publication Request
( ) Other: _____

CLAIMS AS FILED

FOR	NO. FILED	NO. EXTRA	RATE	FEE
Total Claims	20	0	$ 25.00	$ 0.00
Independent Claims	5	2	$100.00	$ 200.00
Multiple Dependent Claims (if applicable)				$ 0.00
Basic Filing Fee				$ 150.00
Utility Search Fee				$ 250.00
Utility Examination Fee				$ 100.00
Assignment Recording Fee				$ .00
Total Fee				**$ 700.00**

At any time during the pendency of this application, please charge any fees required or credit any overpayment to Deposit Account No. 50-0685 (Order No. RAD2P001).

Respectfully submitted,

By: _____
William J. James, Reg. No. 40,661

Date: September 27, 2005

Correspondence Address:

Customer No. 21912
Van Pelt, Yi & James LLP
10050 N. Foothill Blvd. Suite 200
Cupertino, CA 95014
Phone: 408-973-2585

I hereby certify that this is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated below and is addressed to:

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

By: _____

Typed Name: Veronica Pula

Express Mail Label No.: EV323820157US

Date of Deposit: September 27, 2005

Attorney Docket No. RAD2P001

APPLICATION FOR UNITED STATES PATENT

CONTAGION ISOLATION AND INOCULATION

By Inventors:

James A. Roskind
920 Governors Bay Drive, Redwood City CA 94065
A Citizen of the United States of America

Aaron T. Emigh
762 Judith Court, Incline Village NV 89451
A Citizen of the United States of America

Assignee: Radix Labs, LLC

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Telephone (408) 973-2585

CONTAGION ISOLATION AND INOCULATION

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 60/613,909 (Applicant Docket No. RJ-025) entitled CONTAGION ISOLATION AND INOCULATION filed September 27, 2004, which is incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] Laptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization; and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person. Similarly, a stationary system may become infected, e.g., due to receipt and execution of malicious code via a network or other communication and/or a diskette and/or other removable media. Upon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm.

Ex.1002
NETSKOPE, INC. / Page 308 of 378

Therefore, there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network.

Ex.1002
NETSKOPE, INC. / Page 309 of 378

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] Figure 1 is a flow diagram of a method for reducing an anti-contagion update interval during periods of suspicious network activity according to some embodiments.

[0005] Figure 2A is a flow diagram of a method for cooperatively scheduling an anti-contagion update interval according to some embodiments.

[0006] Figure 2B is a block diagram of a network environment in which anti-contagion updates are distributed according to some embodiments.

[0007] Figure 3A is a flow diagram of a method for contacting an anti-contagion source and optionally getting an update according to some embodiments.

[0008] Figures 3B-3D illustrate distributed update distribution as implemented according to some embodiments.

[0009] Figure 4A is a flow diagram of a method for acquiring an update according to some embodiments.

[0010] Figure 4B is a block diagram of a client system configured to obtain an update according to some embodiments.

[0011] Figure 4C is a block diagram of a system used to distribute an update according to some embodiments.

[0012] Figure 5 is a flow diagram of a method for distributing updates according to some embodiments.

Ex.1002
NETSKOPE, INC. / Page 310 of 378

[0013] Figure 6 is a flow diagram of a method for establishing a redistribution policy according to some embodiments.

[0014] Figure 7 is a flow diagram of a method for redistributing content such as updates according to some embodiments.

[0015] Figure 8 is a flow diagram of a method for using peers or other indirect data sources to acquire content such as updates according to some embodiments.

[0016] Figure 9 is a flow diagram of a method for redistributing content such as updates according to some embodiments.

[0017] Figure 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments.

[0018] Figure 10B is a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined according to some embodiments.

[0019] Figure 11 is a flow diagram of a method for identifying vulnerabilities according to some embodiments.

[0020] Figure 12 is a flow diagram of a method for identifying an infestation according to some embodiments.

[0021] Figure 13 is a flow diagram of a method for monitoring one or more computers for infestation according to some embodiments.

[0022] Figure 14 is a flow diagram of a method for quarantining a computer according to some embodiments.

[0023] Figure 15 is a flow diagram of a method for quarantining a computer according to some embodiments.

[0024] Figure 16 is a flow diagram of a method for a quarantine server to respond to requests according to some embodiments.

Ex.1002
NETSKOPE, INC. / Page 311 of 378

[0025] Figure 17 is a flow diagram of a method for scanning backdoors and inoculating according to some embodiments.

[0026] Figure 18 is a flow diagram of a method for categorizing messages according to some embodiments.

[0027] Figure 19A is a flow diagram of a method for notifying possible sources of infection according to some embodiments.

[0028] Figure 19B is a block diagram illustrating a network environment in which suspicious messages are identified and/or one or more notifications are sent when a malicious message is detected.

Ex.1002
NETSKOPE, INC. / Page 312 of 378

DETAILED DESCRIPTION

[0029] The invention can be implemented in numerous ways, including as a process, an apparatus, a system, a composition of matter, a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. A component such as a processor or a memory described as being configured to perform a task includes both a general component that is temporarily configured to perform the task at a given time and a specific component that is manufactured to perform the task. In general, the order of the steps of disclosed processes may be altered within the scope of the invention.

[0030] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0031] Contagion isolation and inoculation is disclosed. In some embodiments, a request is received from a host, e.g., via a network interface, to connect to a protected network. It is determined whether the host is required to be quarantined. If the host is required to be quarantined, the host is provided only limited access to the protected network. In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed,

Ex.1002
NETSKOPE, INC. / Page 313 of 378

such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed. In various embodiments attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user.

[0032] Contagion refers herein to software programs and/or code, data values, configurations, and settings, that expose a computer or other system to security threats, such as unauthorized access and/or use of the system and/or data stored thereon; corruption or loss of data; and/or damage, loss, and/or unauthorized reconfiguration of system software and/or hardware components. Examples of contagion include software programs and/or code designed to perform undesirable and/or unauthorized actions from the perspective of the (authorized) user of a computer, and at the same time perform desired actions from the perspective of the creator or controller of such contagion. Examples of contagion include computer worms, viruses, and Trojan horses. Anti-contagion software refers herein to software that prevents, impedes or remediates contagion, such as Norton Antivirus from Symantec, or VirusScan from McAfee, which identifies and/or removes contagion from a user's computer. Another example of anti-contagion software is software that repairs a security vulnerability through which contagion may spread. Many anti-contagion methods rely on contagion descriptions, such as virus signatures, to identify the contagion, and must be updated regularly to be effective.

[0033] Figure 1 is a flow diagram of a method for reducing an anti-contagion update interval during periods of suspicious network activity according to some embodiments. An update interval refers herein to a period of time between acquisition of updates, such as security updates, virus signature file updates, or virus scanner updates. In this example, network traffic statistics may be monitored (101). An example of traffic statistics is latency experienced by email, such as average latency, or median latency. Another example of traffic statistics is the rate of unacceptable attempted TCP/IP traffic,

Ex.1002
NETSKOPE, INC. / Page 314 of 378

such as attempts to connect to blocked or restricted ports, or insufficiently authenticated (or authorized) connections to ports, or connections that provided invalid or illegal content such as extraordinarily long strings, or specific content detected to be malicious. Recent activity may be evaluated (102) to see if it is anomalous. Examples of anomalous activity include median email latency in mail queues beyond some threshold, for example above a 4 hour median queuing delay, and rates of unacceptable attempted TCP/IP traffic beyond some threshold, for example greater than two attempts per minutes over a one hour period. Another example of a threshold for anomalous activity is a comparison with recent historical statistics, such as unacceptable attempted TCP/IP traffic at a rate greater than ten times the expected rate over a 30 minute period. The expected rate may for example be an average over a recent historic period, such as an average rate over the last week of connectivity. If activity is not deemed anomalous (103), then in this example, processing continues with no change (104) in the next update interval. If the activity is deemed anomalous (103), then in this example, the next update interval is reduced, for example reduced to some proportion of the planned update interval, for example reduced to 25% of the previous or default update interval. Another example of reducing the next update interval is to reduce the currently remaining time until an update, for example reducing by a proportion, such as 50%, the remaining time until an update is requested.

[0034] Figure 2A is a flow diagram of a method for cooperatively scheduling an anti-contagion update interval according to some embodiments. In this example, the planned time for contacting an anti-contagion source may arrive (201). An old version identifier may be retrieved (202), such as a checksum or hash for a file, or a version number for software stored in a file system or registry, or a version number for an anti-virus signature file stored in a file system or registry. An update may be requested from an anti-contagion source (203), for example as is discussed in conjunction with Figure 3A, which may include updating or concluding that an update is not needed. A time for next contacting an anti-contagion source is decided upon (204). In some embodiments, the scheduled time may be made sooner when the source of the update, such as a vendor of software to which the update pertains, anticipates the impending release of a fully tested update, such as scheduling a next contact time in a few hours, or a few days. If the

Ex.1002
NETSKOPE, INC. / Page 315 of 378

current computer's version of anti-contagion software contains resolutions to all known problems and otherwise anomalous traffic patterns then, in this example, the update interval may be made longer, such as the full default interval for a computer, for example one week. In some embodiments, the selection of the next update interval may be dependent on the specific product. For example, a "pro version" may have a short default interval, such as one day, and a "home version" may have a relatively long default interval, such as two weeks or one month.

[0035] Figure 2B is a block diagram of a network environment in which anti-contagion updates are distributed according to some embodiments. A plurality of clients 1 to "n", represented in Figure 2B by clients 220, 222, and 224, are connected to the Internet 226. An update server 228 also is connected to the Internet 226. In various embodiments, one or more of the clients 220-224 is configured to request and obtain updates, if any, from update server 228 via the Internet, e.g., as described above in connection with Figure 2A.

[0036] Figure 3A is a flow diagram of a method for contacting an anti-contagion source and optionally getting an update according to some embodiments. In this example, an old version identifier may be retrieved (301), for example as was discussed in 202 of Figure 2A. Contact may be made with an anti-contagion source (302) via a network such as the Internet. The old version identifier may be provided, for example using a transport protocol such as TCP/IP, and a data encapsulation format such as XML, or using a higher level protocol and format such as SOAP. A decision may be made as to whether an update is needed (303). In some embodiments, this update decision may be made by a server, upon review of the old version identifier. In some embodiments, this update decision may be made by the user's computer. In some embodiments, the update decision may be made by incorporating preferences held on a user's computer, such as a preference to always have the newest updates, or preferences to avoid updates that have been available for less than a threshold length of time (for example, 2 weeks), or preferences that accept an additional update when the source indicates urgency associated with the update. In some embodiments, the update decision may be made based on

Ex.1002
NETSKOPE, INC. / Page 316 of 378

considerations such as the size of the potential update, for example by avoiding the overhead of small updates, and only performing an update when a threshold amount of change has taken place, or when a threshold length of time has elapsed since an actual update was made. An example of a threshold amount of change taking place is the addition of a prescribed number of viral signatures, such as 2 new signatures. An example of a threshold length of time is 3 weeks. If the update is not needed (303) then the process of contacting the source is complete (304) in this example. If an update is needed (303) then an update is acquired in this example via direct or indirect channels (305), for example as further described in conjunction with Figure 4A. After the update has been acquired (305), the contact may be complete (306).

[0037] Distributed update distribution is disclosed. In some embodiments, at least some users receive an update indirectly, e.g., from another user that received it previously, either directly from the original source or indirectly from a source that had itself earlier received it, again either directly or indirectly, and so on. Figures 3B-3D illustrate distributed update distribution as implemented according to some embodiments. In the example shown in Figures 3B-3D, it is assumed for expository purposes that each host that receives the update will serve as a redistribution node, each recipient has the ability to redistribute at the same rate as the original source, and there is continuous demand for the update from all sources. As shown in Figure 3B, at a time t1 a first direct recipient of the update D1 (332) downloads the update from the original source S1 (330). As shown in Figure 3C, at a time t2 a second direct recipient D2 (334) downloads the update from the original source and an indirect recipient R11 (336) downloads the update from the first direct recipient D1 (332), which in this case acts as a redistribution node. As shown in Figure 3D, at a time t3 a third direct recipient D3 (338) downloads the update from original source S (330), a second indirect recipient R12 (340) downloads the update from the first direct recipient D1 (332), a third indirect recipient R21 (342) downloads the update from the second direct recipient D2, and a fourth indirect recipient R111 (344) downloads the update from first indirect recipient R11 (336). In this example, in the three download cycles shown in Figures 3B-3D on its own the original source would only have been able to download the update to the three direct recipients,

Ex.1002
NETSKOPE, INC. / Page 317 of 378

but by using previous recipients to redistribute, in the example shown in Figures 3B-3D a total of seven recipients have been able to obtain the update. In a generalized case, under the assumptions used in this example in "n" download cycles/periods a total of 2^n-1 recipients are able to obtain the update, whereas only "n" recipients, i.e., one per cycle, would otherwise have been able to obtain the update if it were only available directly from the original source. In an even more generalized case, under an assumption that each server may download roughly k copies in a time interval, for example where more than one download is provided by a server at a time, then in "n" download cycles (or periods) a total of roughly $(k+1)^n$-1 recipients are able to obtain the update, where as only k*n recipients, i.e., k per cycle, would otherwise have been able to obtain the update if it were only available directly from the original source.

[0038] Figure 4A is a flow diagram of a method for acquiring an update according to some embodiments. In this example, an update source is contacted (401), such as via an Internet connection, for example via TCP/IP. An offer to serve as a redistribution source is made (402). In some embodiments, a redistribution source may be contacted by other computers to acquire an update. An example of an offer to be a redistribution server is described in conjunction with Figure 6. In various embodiments, 402 is optional, performed only if a criterion or test is satisfied, or omitted. An update or an update identifier is acquired (403). An example of an update identifier is a version number for an update. Another example of an update identifier is a checksum for an update. Another example of an update identifier is a set of checksums (such as MD5, SHA-1, or CRC-32) for a corresponding set of byte ranges that form the update. Another example of an update identifier is a combination two or more identifiers, such as the identifiers enumerated above. If the update was completed (404) then the user confirms redistribution sourcing status (408) in this example. In some embodiments, confirmation includes asserting that the client is prepared to redistribute copies of the received data to one or more recipients. If the update was not completed (404), then a list of peer or other sources is acquired (405) in this example. In some embodiments, the list is or may be explicit. In some embodiments, the list is or may be implicit, for example represented by an iterator or accessor, which may retrieve elements on an as needed basis. In some

Ex.1002
NETSKOPE, INC. / Page 318 of 378

embodiments, implicit lists are dynamic, and calculated or created in part on an as needed or as requested basis. In some embodiments, the list of other sources contain addresses that may be contacted to acquire an update, such as a list of IP addresses and ports, as well as optionally some authentication information to be used when contacting a listed source. In some embodiments, a requesting host that agrees to serve as a redistribution source is provided with a list of sources from which the update is available immediately, or at least sooner than it will be made available to hosts that will not redistribute. One or more attempts may be made to acquire the update from a listed source (406), for example as exemplified in Figure 8. If the update is completed via a listed source (407), then redistribution status is confirmed (408) in this example. If the update is not complete (407) then a reservation is optionally negotiated and/or acquired (409) in this example. In some embodiments, a reservation may include a time and/or a specific source or IP address. In some embodiments, a reservation address may be selected from a collection of source addresses, for example in order to distribute the load across more than one server, or to provide a server that is closer to a recipient. An example of selecting a server close to a recipient is to select a server having relatively lower latency during a download, or relatively lower cost, for example by selecting a source within a recipient's ISP complex or within a recipient's intranet or home network. If a reservation time was acquired, then a wait for that reservation time (410) is performed in this example. At the reservation time, a further attempt to acquire an update or update identifier from the source (403) is made, and the flow proceeds as described earlier. This flow may continue until an acquisition is complete (408), as also described earlier. In various embodiments, one or more of confirming redistribution sourcing status (408), attempting to obtain the update from a redistribution source (405-407), and/or acquiring and/or waiting for a reservation time (409-410) is/are optional, conditional, or omitted.

[0039] Figure 4B is a block diagram of a client system configured to obtain an update according to some embodiments. In some embodiments, the client system shown in Figure 4B is used to implement one or more of clients 220-224 of Figure 2B. The client system 420 includes a communication interface 422, such as a network interface card, configured to send/receive communications via a network, such as the Internet. The

Ex.1002
NETSKOPE, INC. / Page 319 of 378

client system 420 further includes an update agent and/or browser 424. In some embodiments, the update agent/browser 424 comprises browser software used to navigate the World Wide Web, e.g., to send/receive data to/from a website from which an update is available for download. In some embodiments, update agent/browser 424 includes an agent associated with anti-contagion software installed on the client system 420. In various embodiments, the update agent/browser 424 comprises one or more components and is implemented as one or more software programs running on a processor and/or one or more hardware components. A settings data store 426 stores one or more settings and/or other data associated with the software with which an update and/or software to which the update does or may pertain, such as periodicity or next scheduled (e.g., reservation) time to check for updates, a list of update identifiers, locators, and/or redistribution sources from which an update is or may be available, policies for whether and/or under what terms, conditions, circumstances, etc. the client system 420 may be used redistribute an update, a last update time, an old version identifier (see, e.g., 202 of Figure 2A), etc.

[0040] Figure 4C is a block diagram of a system used to distribute an update according to some embodiments. In some embodiments, the system of Figure 4C is used to provide an update server, such as update server 228 of Figure 2B. In this example, the distribution system 440 includes a communication interface 442 configured to send/receive data via a network, such as the Internet. An update distribution engine 444 is configured to receive and service requests for updates. For updates provided directly to a request source, the update distribution engine 444 obtains the update from an update storage location 446 and provides the update to the request source via the communication interface 442. In some embodiments, if data included in the request indicates the source of the request is or may be willing to serve as a redistribution source, the update distribution engine 444 hands the request off to a redistribution coordinator 448, which negotiates with the request source, e.g., based on policies, settings, rules, etc. stored in a policies and lists data store 450, through communications sent/received via communication interface 442, to determine if the requesting source will serve as a redistribution source and, if so, to determine the terms and conditions of such service and

Ex.1002
NETSKOPE, INC. / Page 320 of 378

data, such as an address, locator, or identifier, that can be provided to other requesting systems and/or users to enable them to attempt to obtain the update from the redistribution source. In some embodiments, if update distribution engine 444 determines that it is not able to provide the update to the request source directly (e.g., due to capacity limits or because a policy applicable to the request and/or the request source indicates the request source should be directed to a redistribution source, e.g., because the request source has a less expensive version of the software or is not willing to serve as a redistribution source), the update distribution engine 444 hands the request off to redistribution coordinator 448, which provides to the request source an update identifier and a list of one or more redistribution sources from which the update is or may be available to the request source.

[0041] Figure 5 is a flow diagram of a method for distributing updates according to some embodiments. In this example, a source prepares to supply updates to recipients (501), for example by starting up a server, for example an HTTP or FTP server, or a multicast server, such as an RTP multicast server. The server waits for an event (502), such as a contact on a predefined port, or a notification that the server should start a multicast. If a multicast-time event appears (503) then an update is multicast (504) in this example. In some embodiments, a multicast time event may be generated internally or externally to the server to start a multicast. In some embodiments, a multicast-time event may be automatically generated at predetermined times, such as hourly, weekly, or daily, or on individually specified dates and times. In some embodiments, a multicast-time event may include a specific identifier for the multicast. If an event of the form of an update request arrives (503) then a test for authenticity is optionally performed (505) in this example. An example of determining whether a request is authentic is to check a credential. Examples of credentials include a provided shared secret, such as a secret used by all requestors to this server, or a different secret used by each requestor such as a user serial number, or a cryptographically signed authentication, such as credentials or a certificate issued to users that had paid for an update service, for example, by inclusion in a purchased software package. In some embodiments, all requests are assumed to be authentic without the use of any authenticator. If the request was not authentic (505)

Ex.1002
NETSKOPE, INC. / Page 321 of 378

then, in this example, the server continues to wait for an event (502). If the request was authentic (505) then the server may determine a necessary update (506) in this example. In some embodiments, determination of an update may be made based on the requestor's state, which in some embodiments may be indicated in a received request for update. A redistribution contract may be negotiated (507). In some embodiments, some requestors may agree to redistribute updates to other requestors. In some embodiments, some requestors may decline to redistribute updates. In some embodiments, a source may decline redistribution proposals from a requestor. An example of a redistribution contract is an agreement not to redistribute. Another example of a redistribution contract is an agreement to redistribute a fixed number of copies, such as five copies. Another example of a redistribution contract is an agreement to redistribute for a fixed period of time, such as one day. Another example of a redistribution contract is an agreement to redistribute within a specified geographic region within a fixed period of time. Another example of a redistribution contract is an agreement to redistribute indefinitely, for example until a replacement update is provided. A redistribution contract may be made with terms that are combinations of the above mentioned exemplary term limitations. An update may be provided directly or indirectly (508). A direct update may for example be provided by allowing an FTP download, or by encapsulating the transmission in an HTTP transfer, for example using XML and/or an appropriate coding, such as uuencode. An indirect update may be provided by directing the requestor to an alternate source, such as a redistribution server, or a server at a different address, or a server at a different time, such as a future time, or a combination of two or more such specifications. In some embodiments, a decision to provide direct vs. indirect updates may be based in part on the redistribution contract, for example a requestor that is willing to redistribute may be updated sooner or more directly. An example of a redistribution contract is a promise by a user to provide redistribution in exchange for purchase price concession, such as a reduced initial purchase price, or a quantity discount price. In some embodiments, a decision to provide direct vs. indirect updates may be based in part on previous agreements, such as prepayment for expedited service, such as may be included in a more expensive version of a product that utilizes the updates. The server may wait for an event (502). In some

Ex.1002
NETSKOPE, INC. / Page 322 of 378

embodiments, events may be processed in parallel with previous events, or may be sequentially processed, or some combination, for example up to a threshold number of events in parallel, such as a maximum of 32 events in parallel.

[0042] Figure 6 is a flow diagram of a method for establishing a redistribution policy according to some embodiments. In this example, a computer may prepare to offer to be a redistribution source (601). In some embodiments, preparations may include retrieving preferences, such as the number of redistributions that may be done, or the duration of time that the computer is willing to act as a redistribution source. In some embodiments, preferences may be defaults, or may be configured by a user and stored persistently, such as in a registry or file system. A contact address may be proposed to the source and a policy may be negotiated (602). A contact address may for example be a globally routable IP address and a port, or a local IP address (reachable from a LAN behind a firewall) and port that can be accessed by other computers on the LAN, such as computers that shared a common NAT address in their contact with the original source. In some embodiments, negotiation may include proposing a policy. In some embodiments, negotiations may involve a counter proposal in response to a proposal. An example of a counter proposal criterion is to require a minimum duration for redistribution. If terms were not acceptable (603) then, in this example, the computer does nothing (604). If the terms were acceptable (603) then, in this example, the computer prepares to service redistribution requests (605), for example by establishing a server to respond at the agreed contact address, reserving storage to hold the content for redistribution, etc. In some embodiments, redistribution policy may be a broader contractual matter, where an update is provided more quickly or more directly in exchange for a promise to redistribute. In some embodiments, an auditing mechanism may be used to measure compliance and penalize contract breakers, such as failure to accept connections for redistribution, where penalties may for example include refusal to accept future similar contracts. As another example, a lower purchase or subscription price may be offered for operators of a software product, such as antivirus software, who agree to act as redistribution points. In some embodiments such purchase agreements

Ex.1002
NETSKOPE, INC. / Page 323 of 378

may be configured into the software, for example by establishing agreements to act as a redistribution point for updates as defaults that a user cannot modify.

[0043] Figure 7 is a flow diagram of a method for redistributing content such as updates according to some embodiments. In this example, a redistribution computer is contacted and confirms its sourcing status (701), for example by accepting a TCP/IP connection on a predefined port, and processing a request for content. The redistribution computer may optionally contact another computer, for example a more original source, and affirm its redistribution sourcing status (702). A more original source may be a source that has provided content in the past to the redistribution computer, directly or indirectly. In some embodiments, contacting a more original source demonstrates that the redistribution computer is performing redistribution. In some embodiments, contacting a more original source allows the redistribution computer to further authenticate the computer that requested the content, for example by getting confirmation from a more original source that a specific computer was authorized to request the content. An authentication to be used to authenticate requests is negotiated (703). In some embodiments, authentication includes providing a shared secret to the redistribution computer. In some embodiments, authentication includes presenting an authorization cryptographically signed by a more original source, such as a certificate. In some embodiments, all requests are presumed authentic. If the request is not authentic (704), then nothing further is done (705) in this example. If the request is authentic (704), then the requested update is supplied (706) in this example. The updates may be supplied for example via a transport protocol TCP/IP, or a higher level protocol such as FTP, HTTP, or HTTPS, etc.

[0044] Figure 8 is a flow diagram of a method for using peers or other indirect data sources to acquire content such as updates according to some embodiments. In this example, a list of one or more peers or other indirect sources for acquiring updates is obtained (801), for example as was discussed in conjunction with 405 of Figure 4A. In one example, an indirect source may be a peer, such as another computer that has downloaded the content. In another example, an indirect source may be a computer

Ex.1002
NETSKOPE, INC. / Page 324 of 378

configured to redistribute content without other use of the content, such as an ISP server established to redistribute content to subscribers. In another example, an indirect source may be a server created or authorized by the original source to perform additional distributions. In some embodiments, an obtained list of indirect sources may be implicit, for example by referring to a list using an iterator or accessor construct that can itemize entries in the list when requested, for example using a query to a service when an additional item in the list is required, which may for example dynamically complete the list on an as requested basis. A next address and (optional) authenticator in the list of sources is retrieved (802). Any order may be used. In some embodiments, an order of processing may correspond to the original list order. In some embodiments, an order of processing may be such that the earlier processed addresses would be expected to have lower latency and/or higher bandwidth, for example by first processing a local address on a LAN. In some embodiments, elements of the list are or may be processed in parallel, and portions (such as byte ranges) of the content may be acquired from different addresses in the list. An address on the list may be contacted to request content (803), which may in some embodiments be performed as described in conjunction with Figure 7. In one example, a source address may consist of an identifier for a broadcast with optional time(s) for a broadcast, and contact with the source may include receiving the broadcast. In another example, contact with the source may include making a connection such as a TCP/IP connection with the source. If the acquisition is complete (804), then the processing is complete (805) in this example. If the acquisition was not completed (804) then additional sources in the list are considered in this example. If there are more sources in the list (806) then, in this example, a next source is retrieved along with an optional authenticator (802) and the processing continues. If there are no more sources (806) then the attempted acquisition from source(s) is unsuccessful (807) in this example.

[0045] Figure 9 is a flow diagram of a method for redistributing content such as updates according to some embodiments. In this example, a computer prepares to supply content (or updates) to a requestor/recipient (901), for example by starting up one or more servers. Examples of a server include an HTTP server, an FTP server, and a

Ex.1002
NETSKOPE, INC. / Page 325 of 378

multicast server. A server waits for an event (902), such as a contact on a predefined port, or a notification that the server should be terminated, or a notification that a time for a multicast has arrived. If a service expiration event appears (904) then the supply service is terminated (905) in this example. A service expiration event may be automatically generated, for example after a predetermined duration of service, or after a predetermined number of copies of an update have been redistributed. If a request event arrives (904), then a test for authenticity is performed (906) in this example. Authenticity may be established in the request, for example by receiving and validating, or performing a mutual proof of possession of, a shared secret, such as a secret used by all requestors to this server, or a different secret used by each requestor of this service and held in a list of single-use secrets by this server, or by providing a cryptographically signed authentication. In some embodiments, all requests are considered authentic without the use of any authenticator. If the request was not authentic (906) then, in this example, the server continues to wait for an event (902) as described earlier. If the request was authentic (906) then, in this example, the server transmits a copy of the content to the requestor (907), for example by allowing an FTP download, or by encapsulating the transmission in an HTTP transfer, for example using XML and/or an appropriate coding, such as uuencode.

[0046] Figure 10A is a flow diagram of a method for identifying and remedying problems according to some embodiments. A problem may be identified as some event or status that may cause direct or potential harm. Exemplary problems include vulnerability or infestation. In this example, a problem such as a vulnerability or infestation is detected (1001). Infestation herein refers to the current presence and/or execution of contagion. In some embodiments, detection may be made by a router, firewall, or other network component, separately or in concert, using techniques such as those illustrated by Figures 11, 12, and 13. In some embodiments, detection may be made by a computing device, for example a computing device operated by an ISP. After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other

Ex.1002
NETSKOPE, INC. / Page 326 of 378

computers, or efforts to communicate data without authorization, including for example file contents and keyboard entry logs. In some embodiments, no communications are authorized. In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in Figure 14 and 15. In this example, the quarantined computer is provided access to remediation services (1003). In some embodiments, access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools. In some embodiments, access to remediation includes allowing direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained. In some embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, certain content requests, such as specific URLs or specific file downloads. In some embodiments, remediation content may be substituted for other requested content, for example as discussed in conjunction with Figure 14.

[0047] Figure 10B is a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined according to some embodiments. A plurality of hosts 1 to "m", represented in Figure 10B by hosts 1020, 1022, and 1024, connect via a router 1026 and a gateway 1028 to the Internet 1030. In various embodiments the router 1026 is omitted or included in the gateway 1028. In various embodiments, gateway 1028 comprises a gateway, router, firewall, or other device configured to provide and control access between a protected network and the Internet and/or another public or private network. In various embodiments, the process of Figure 10A is implemented, in the event of quarantine of one or more of hosts 1020-1024, for example, on the affected (quarantined) host, router 1026, and/or gateway 1028. In some embodiments, a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server 1032, e.g., to download a patch,

Ex.1002
NETSKOPE, INC. / Page 327 of 378

more current threat definition, etc. In some embodiments, requests to connection to a host other than the remediation server 1032 are redirected to a quarantine server 1034 configured to provide a notice and/or other information and/or instructions to a user of the quarantined host. In various alternative embodiments the quarantine server 1034 is omitted or resides on the router 1026 and/or gateway 1028.

[0048] Figure 11 is a flow diagram of a method for identifying vulnerabilities according to some embodiments. In this example, preparation is made to scan for one or more vulnerabilities (1101), for example by retrieving one or more IP addresses of computers that need to be scanned. For example, an IP address may be provided by a DHCP sever hosted in an ISP network complex, to identify current subscriber IP addresses. As another example, a subnet range may be scanned, for example by taking an address of the form A.B.C.X, and using some or all values of X in the range 0 to 255 to enumerate distinct IP addresses. A scan of one or more IP addresses may optionally be performed to detect an open port (1102). An example of scanning an IP address is scanning to detect open TCP/IP ports (1102). An open port may be identified by attempting to form a connection, such as a TCP/IP connection to that port. In some embodiments, only open ports on a given computer will provide acknowledgment messages needed to establish a TCP/IP connections, which for example causes a success code to be returned by Unix "connect()," and a closed port will provide no response to the attempt to connect, which for example would cause an error code to be returned by the Unix function call "connect()". If no open ports are detected (1103), then the scanning is complete (1106) in this example. If open ports are detected (1103) then those ports are tested for vulnerabilities (1104) in this example. In some embodiments, an open port is assumed (1103) and a test for vulnerability is performed or attempted (1104), for example by communicating a vulnerability test without independently testing to see if one or more requisite ports are open. In some embodiments, a vulnerability test of a port may include sending data that is known to create a discernable response when a vulnerability is present, such as sending a long string known to induce a buffer overflow with a consequent errant response, where the errant response may for example include a characteristic communication, premature termination of the connection, or other

Ex.1002
NETSKOPE, INC. / Page 328 of 378

erroneous response(s). In some embodiments, a test for a vulnerability is an attempt to exercise a service, such as a sendmail or an RPC service, in search of a misconfiguration of that service that creates a vulnerability. One example of a misconfiguration of a service is provision of any such service. Another example of a misconfigured service is one where a password should be required for security purposes, but no password is required by the misconfiguration. Another example of a misconfiguration is the use of an easily guessable password, such as the default installation password, when resulting access creates a security vulnerability. Another example of a misconfigured service is support for a service provided by an unauthorized agent, such as a worm or virus. If no vulnerabilities are detected (1105) then scanning is complete (1106) in this example. If vulnerabilities are detected (1105) then an associated IP address is flagged as vulnerable (1107) in this example. In the case of a subscriber to an ISP, an IP address may be translated to a particular subscriber identity, for example by checking in DHCP or static IP allocation tables for the subscriber's identity, or for example by extracting a MAC address from traffic associated with the IP address, and such identity may be appropriately flagged or recorded. In some embodiments, the record of the vulnerability may additionally include the port, and the details of the vulnerability that was detected, such as which buffer overrun was vulnerable, or which service was misconfigured to create a vulnerability.

[0049] Figure 12 is a flow diagram of a method for identifying an infestation according to some embodiments. In this example, a device near a computer, such as a firewall on a LAN or an ISP's router, is used in some embodiments to monitor a computer for infestation (1201). Network traffic is monitored for anomalous traffic volume, port, or IP destination (1202), for example by detecting large volumes of outbound traffic, such as email traffic or instant messaging traffic. Another example of anomalous traffic is a TCP/IP connection to a server that is known to control a collection of infested machines, in a way that suggests the connecting machine is controlled by the server, such as connecting and transmitting an assertion that it is controlled or available to comply. Another example of anomalous traffic is a connection to a computer that is a current target of a denial of service attack, with a pattern that is consistent with the attack,

Ex.1002
NETSKOPE, INC. / Page 329 of 378

such as a connection to a targeted port, or the use of a falsified return IP address. In some embodiments, a falsified return address may be detected by a router, such as an ISP router, that is aware that the return address is not on the sourcing subnet, or not associated with the MAC address that has supplied the corresponding packets. If an anomaly is detected (1203) then an apparent infestation is noted (1204) in this example. In some embodiments, a response to infestation may include quarantining of the computer or network containing the computer, for example as discussed in conjunction with Figures 14, 15, and 16. In some embodiments, a response to infestation may include an attempt to remediate the problem, for example by inoculation, such as discussed in conjunction with Figure 17. If no anomaly is detected (1203) then monitoring is complete (1205) in this example. In some embodiments, monitoring for anomalous traffic may be continuous. In some embodiments, monitoring for anomalous traffic may be periodic. For example, periodic monitoring may consist of monitoring some number of computers, such as 1 computer, for some period of time, such as 2 minutes, and then not monitoring those computers again for another period of time, such as 1 hour. As another example, periodic monitoring may be randomized, for example by changing the duration of monitoring, pattern of selecting computers to monitor, and/or the unmonitored duration, to be difficult or impossible to predict, for example by being driven by a pseudo random number generator, subject to restrictions of available monitoring computers.

[0050] Figure 13 is a flow diagram of a method for monitoring one or more computers for infestation according to some embodiments. In this example monitoring of a computer for infestation begins (1301), for example by retrieving a list of one or more addresses of computers, such as addresses of participating subscribers. In some embodiments, this list may be a list of addresses for some or all subscribers for a given ISP. In some embodiments, the list may be a list of IP addresses issued by a DHCP server, such as on a LAN, or a list of IP addresses observed by a router, such as a router on a LAN, or a complete list of IP addresses in a given subnet. A computer associated with an address identified in a list is queried for a cleanliness assertion (1302), for example by contacting a trusted computing base within a computer, and requesting an authenticated infestation scan by trusted software. An example of a trusted computing

Ex.1002
NETSKOPE, INC. / Page 330 of 378

base within a computer is the Paladium security initiative under development by Microsoft and supported by Intel and American Micro Devices. Another example of a trusted computing base is described in various TCG specifications, such as the TCG Architecture Overview, published by the Trusted Computing Group. Trusted code bases may for example execute antivirus scans of the remainder of the computer, including untrusted portions of the disk and/or operating system. In some embodiments, trusted code bases may digitally sign assertions about the cleanliness (e.g. infestation status) and/or state of their computers. In some embodiments, the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan, such as the last time a scan was performed, or a version associated with a current anti-contagion software or definition file in use, wherein a sufficiently updated software and/or scan may act as a cleanliness assertion. In some embodiments, an operating system may respond with information associated with its patch level, wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness. If a computer asserts it is clean (1303) then monitoring is complete (1305) in this example. If a cleanliness assertion is not provided (1303) then an infestation or vulnerability is presumed (1304) in this example.

[0051] Figure 14 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1401), such as an ISP deciding to quarantine a subscriber, or a firewall or router for a LAN deciding to quarantine a local computer. In some embodiments, a decision to quarantine may be made based on apparent infestations or apparent vulnerabilities, for example as illustrated in conjunction with Figures 11, 12, or 13. In some embodiments a decision to quarantine may be based on the accumulation of evidence above a threshold, such as a threshold of one such piece of evidence, or a threshold of two such pieces of evidence. In some embodiments, a decision to quarantine may be made based on configuration rules, for example all new computers must be quarantined until they have contacted their OS vendor and been updated, or by user specification, such as a user requesting a quarantine for a specific computer. In some embodiments, requests for a quarantine may be made on an individual computer via

Ex.1002
NETSKOPE, INC. / Page 331 of 378

settings, such as control panel in Microsoft Windows, or through a user interface to a firewall or router, for example by specifying an IP address, name, or MAC address to quarantine, or a list of addresses that are not to be quarantined (where other addresses may be quarantined). During a quarantine period outbound traffic is detected (1402), for example by a device such as a router, or by a software network stack on the quarantined computer, or by an upstream device, such as a device at an ISP. Outbound traffic is tested in this example to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact with a security patch update provider, such as Microsoft Windows Update, or contact with a verified remediation site, such as an internal ISP site. If outbound traffic is deemed to be associated with a remediation request (1403), then the traffic is routed or forwarded to its destination (1404) in this example. If outbound traffic is not associated with a remediation request (1403), then, in this example, it is tested to see if it is an approved service request (1405), such as a request for a web page. If the request was for an approved service (1405) then, in this example, the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation. Re-routing of request traffic may be accomplished in numerous ways, for example by providing an alternate DNS service that consistently returns a fixed IP address of a quarantine server in response to all DNS requests. Another example of re-routing a web page request is to respond with a redirect message, which would direct a browser on a quarantined computer to contact a quarantine server that provides remediation information. If the request was not for an approved service (1406), then the outbound traffic is discarded or responded to with in indication that the desired traffic destination is unreachable (1406) in this example.

[0052] Figure 15 is a flow diagram of a method for quarantining a computer according to some embodiments. In this example, a decision has been made to quarantine a computer (1501), for example as described in conjunction with 1401 of Figure 14. Inbound traffic originally destined for a quarantined computer is detected (1502), for example by a network device such as by a router. An example of detecting inbound traffic destined for a quarantined computer is to have a list of quarantined IP

Ex.1002
NETSKOPE, INC. / Page 332 of 378

addresses, and filter or provide additional processing on traffic destined for an address on the list. Detected inbound traffic is tested in this example to see if it is remediation related (1503), such as a response to a remediation request. Direct responses to remediation requests may for example be identified using stateful packet inspection firewall techniques known to those skilled in the art. In various embodiments, at least certain types of traffic from approved sites such as anti-contagion vendors, security update providers, and/or internal ISP sites are deemed remediation related. If traffic is remediation related (1503) then it is forwarded to the quarantined computer (1504) in this example. If traffic is not remediation related (1503) then, in this example, it is discarded or responded to with a message indicating that the destination is unreachable (1507).

[0053] In some embodiments, a configuration based quarantine during an installation of an operating system, such as Microsoft Windows, may be automatically setup, for example by a default installation setting up restrictions in a firewall installed with the OS or by an installation setting defaults for use when network connectivity is enabled, that establishes a quarantine, for example restricting internet connections, for example allowing internet connections only to a security update site such as Microsoft Windows Update. In some embodiments, settings that may establish a quarantine, such as default settings in an operating system installation, may be altered programmatically to remove the quarantine in response to a remediation site, such as a security update service such as Microsoft Windows Update, asserting that there are no other security updates pending. In some embodiments, configuration settings that may establish a quarantine may be altered programmatically to enable a quarantine in response to the presence of one or more security updates, such as provided by an operating system update service such as Microsoft Windows Update, that are available for installation on a computer.

[0054] Figure 16 is a flow diagram of a method for a quarantine server to respond to requests according to some embodiments. In this example, a quarantine server is started (1601), for example by starting a web server, or DNS server, or proxy server, or ftp server, or some combination server. The server waits for a request (1602), for example by listening on a port and waiting for a connection. In some embodiments, a

Ex.1002
NETSKOPE, INC. / Page 333 of 378

device such as a router may forward outbound traffic from a quarantined computer to a quarantine server, for example as illustrated in conjunction with 1407 of Figure 14. If a received connection is a web server request (1603), such as an HTTP request, then the server responds with a quarantine notification page (1604) in this example. An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain. The links on the quarantine notification page may be examples of HTTP addresses that are for use in remediation. Another example of a quarantine notification page is a page that redirects to a quarantine notification page. If the request is not a web server request (1603), then it is tested to see if it is a DNS inquiry (1605) in this example. A DNS inquiry may for example appear on port 53 using TCP/IP or UDP. If the request is not a DNS inquiry (1605) then it may be discarded or responded to as "unreachable" (1606) in this example. If the request is a DNS inquiry (1605) then, in this example, the inquiry is tested to see if it is a DNS request for a remediation host name (1608). A remediation host name may include a host name as appropriate to the reason for a quarantine, such as a host providing anti-contagion software, or a host providing security updates, or a host internal to (or partnered with) an ISP. If the DNS inquiry was for a remediation host name (1608) then the request is proxied to an external DNS service provider (1609) in this example. A proxy to a DNS service (1609) may return a stored or cached response, such as the actual IP address of the host name, or it may contact an external DNS service to relay back the proposed IP address. If the DNS inquiry was not for a remediation host name (1608) then an IP address for a quarantine server is provided (1607) in this example. In some embodiments, when a redirected IP address is provided, such as that of a quarantine server, the DNS response may include a short time to live, for example 0 seconds. A short time to live ensures that a further DNS query will be sent prior to subsequent communications being sent from the quarantined computer to the host that was the subject of the DNS query, aiding a return to normal routing of traffic once the computer is no longer under quarantine. In some embodiments, the server(s) in this example may

Ex.1002
NETSKOPE, INC. / Page 334 of 378

continue to wait for a service request (1602) in parallel with the processing of the requests as described above, or may wait for a service request again after disposition of the previous request as described above.

[0055] Figure 17 is a flow diagram of a method for scanning backdoors and inoculating according to some embodiments. In this example, preparations are made for scanning a computer for a backdoor inoculation path (1701), for example by identifying the computer to be scanned, and enumerating or retrieving a list of one or more backdoors. In one example, an IP address to be scanned may be selected by an ISP from a list of subscribers. In one example, a list of backdoors may include information associated with preloaded software approved by the computer owner for access and inoculation purposes, such as an ISP provided utility that is installed by the subscriber. In some embodiments, an ISP defined backdoor may have an authentication protocol to preclude control by unauthorized parties, such as restrictions on IP address(es) that may contact the backdoor, or shared secrets such as a password required by the sender, or cryptographic authentication such as client authentication on an SSL connection. In some embodiments, a user is requested and/or required to authorize in advance use of an authorized and/or any unauthorized backdoor for purposes of inoculation. As another example, a list of backdoors may include virus or worm installed backdoors, such as those installed by a SubSeven virus or Back Orifice. As another example, backdoors may include exploitable security vulnerabilities, such as a weakness in a web server, or a weakness in an RPC service. A scan may optionally be conducted to detect open TCP/IP backdoor ports (1702) similarly to the scan discussed in conjunction with Figure 11. If none of the backdoors are open (1703), for example there is no response on any of the ports, then the scan is complete (1706) in this example. If one or more backdoor ports are open (1703) then they are tested for usability (1704) in this example. In some embodiments, a backdoor port may be assumed open (1703) and may be tested for usability (1704) without an independent test to see if the port is open. An example of a usability test is no test at all, with the conclusion that a specific port is usable any time it is open. Another example of a usability test is based on the receipt of confirmation of a functional installation of ISP provided backdoor software, such as a confirmation that

Ex.1002
NETSKOPE, INC. / Page 335 of 378

may be provided by the installed software. Another example of a usability test involves the use of a less invasive test of vulnerabilities such a buffer overrun exploit that does not have a permanent impact but provides observable validation (such as a dropped connection). If a backdoor is usable (1705) then the computer is inoculated via a backdoor (1707) in this example. One example of such an inoculation is the remotely controlled download of one or more remedy files into one or more directories, such as an operating system directory, such as the "\windows\system" directory in Microsoft Windows 2000. Another example of an inoculation is the download of an executable file to the computer, followed by the execution of that file. Another example of an inoculation is the download of a data file, such as an anti-contagion signature file, that is interpreted or processed by another executable already on the computer. Another example of an inoculation is the deletion of one or more files from the computer. Another example of an inoculation is the editing of one or more registry entries, or of one or more files, such as deleting, appending or rewriting entries in a registry or file. Another example of inoculation includes a combination of one or more of above techniques, optionally in conjunction with one or more remotely instigated reboot operations. Another example of inoculation includes a combination of one or more of the above techniques, along with an optional dialog box requesting a user's permission to proceed with the inoculation. Another example of inoculation is the use of a dialog box in conjunction with a timer that causes the inoculation to proceed if no user response is given in a prescribed period of time, such as 1 hour.

[0056] Figure 18 is a flow diagram of a method for categorizing messages according to some embodiments. In this example, a message is received (1801), such as an email message or instant message. The purported sender's identity is extracted (1802), for example by examining the "From:" header line in an email message, or by examining the envelope information conveying an email message, or by examining the sender's ID in an instant message. A check is performed to see if the sender has sent any prior messages (1803), for example by scanning an inbox of prior email, or by checking for the sender in a buddy list. If there were no prior messages from the sender (1803) then the message is processed (1804) in this example. Processing the message may for

Ex.1002
NETSKOPE, INC. / Page 336 of 378

example include presenting the message to the user, and/or recording routing information for comparison and categorization of future messages. If there were prior messages from the sender (1803) then routing information used in prior messages is retrieved (1805) in this example. Routing information may for example be extracted from the header in email. Routing information may for example be obtained during an instant message session by retrieving the IP address of the party being communicated with, for example as is done when an instant message session coordinates a peer-to-peer activity such as a direct file transfer with a remote party. In some embodiments, routing information may be stored implicitly, such as in headers of a previously received message, or explicitly, for example by extracting routing information and storing it in a database or file system. Routing information for the current message is compared to prior messages (1806), for example by checking that the IP address for the party being communicated with is in a similar subnet, or allocated within the same geographical region, for example the same continent, as a previous IP address for the same party. IP address to geographical location may be estimated by various software applications and services, such as services provided by MaxMind and described on http://www.maxmind.com. In some embodiments, routing information for an email message may be deduced by examining header information related to mail transfer agents. In some embodiments, similarity in IP addresses for mail transfer agents may be interpreted as implying similar routing. If routing is similar to previous messages from the same sender (1806), then the message is processed as legitimate (1808) in this example. If the routing information for a message purporting to be from a sender is not similar to previous messages from the same sender (1806) then the message is processed as suspicious (1807) in this example. In some embodiments, processing as suspicious may include contributing to a scoring that labels the message as an undesirable message, such as spam, viral, or phishing. In some embodiments, higher probability suspicious messages may be scrutinized further, or may be restricted to some extent in their impact on the computer. An example of restricting impact of a message may include discarding the message. Another example of restricting impact or further scrutiny of a message may include placing a message in a spam inbox. Another example of a restricting impact of a message may include preventing execution

Ex.1002
NETSKOPE, INC. / Page 337 of 378

of content contained in the message, and/or requiring additional user interactions to bypass the restriction, for example by having a user agree to ignore warnings which describe the suspicious circumstances. In various embodiments, the process of Figure 18 is implemented on a mail, messaging, or other server associated with the sender and/or the sender's ISP; a mail, messaging, or other server associated with the recipient and/or the recipient's ISP; and/or one or more intermediate nodes.

[0057] Figure 19A is a flow diagram of a method for notifying possible sources of infection according to some embodiments. In this example, an infected message is received (1901). An example of an infected message is a message classified as such by anti-contagion software. Routing information is extracted from the message (1902). An example of extracting routing information in an email message is to extract header lines inserted by mail transfer agents that propagated the message. Another example of extracting routing information is to acquire an IP address of a party making contact via instant messaging, for example as is provided by AOL's instant message infrastructure for a peer-to-peer file transfer. Routing information from previously received messages is retrieved (1903). An example of retrieving email routing information from prior messages is scanning all received messages, such as messages in an email inbox, and extracting routing information. Another example of retrieving routing information is to query a database or file system where routing information from previous messages has been gathered. Routing information for the infected message is compared with the retrieved routing information (1904). If no similarity with previous messages is found (1904) then in this example a third party notification is made (1906). An example of a third party notification is sending notification to the ISP that provides network access to the message source. Another example of notifying a third party is notifying a viral clearinghouse of the apparent source of a viral message. Another example of a notifying a third party is notifying a service that determines the credibility of a report, such as a collaborative filter service, that accumulates accusations of viral disseminations. In some embodiments, similarity of routing of an infected message with a previous message may include having a previous message from the IP address of the infected message source. If a similarity is found with previous messages (1904) then in this example a notification is

Ex.1002
NETSKOPE, INC. / Page 338 of 378

sent (1905). In some embodiments, notification may be sent (1905) to one or more sources of the prior message(s) that best match the infected message, and/or to third parties. As an example, notification may be sent to an email source that had the same originating IP address as the infected message. In some embodiments, a user may be asked to approve notification(s), for example via a pop-up dialog. In some embodiments, notification may be automatically sent without user intervention.

[0058] Figure 19B is a block diagram illustrating a network environment in which suspicious messages are identified and/or one or more notifications are sent when a malicious message is detected. A message source 1920 sends a message via the Internet 1922 to a message processing system 1926 for delivery via the Internet to one or more message destinations 1924. In various embodiments, the message processing system 1926 comprises a mail or messaging server associated with the message source 1920, a mail or messaging server associated with the destination(s) 1924, and/or an intermediate processing node. In some embodiments, the message source 1920 is connected directly and/or via a local network, and not via the Internet 1922 as shown in Figure 19B, to message processing system 1926. In some embodiments, message processing system 1926 is configured to identify suspicious messages using current and historic routing information, e.g., as described above in connection with Figure 18. In some embodiments, the process of Figure 19A is implemented on message processing system 1926. For example, in some embodiments if message processing system 1926 determines that a message sent by message source 1920 is infected, message processing system 1926 compares routing information associated with the malicious message with corresponding information for one or more messages received previously from the message source 1920. If the routing information is similar, in some embodiments the message processing system 1926 notifies the message source 1920. If the routing information is not similar, in various embodiments the message processing system 1926 notifies the message source 1920, the sender's ISP 1928, and/or a clearinghouse or similar applicable service 1930, as described above.

[0059] Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

[0060] WHAT IS CLAIMED IS:

Ex.1002
NETSKOPE, INC. / Page 340 of 378

CLAIMS

1. A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network;

quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

2. A method as recited in claim 1, wherein detecting an insecure condition includes one or more of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion.

3. A method as recited in claim 1, wherein detecting an insecure condition includes querying the first host for a cleanliness assertion, including by:

contacting a trusted computing base within the first host; and

requesting an authenticated infestation scan by trusted software.

4. A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.

5. A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

6. A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to a remediation host.

Ex.1002
NETSKOPE, INC. / Page 341 of 378

7. A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.

8. A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

9. A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network;

quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and

a memory coupled to the processor and configured to provide instructions to the processor.

10. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion.

11. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by:

contacting a trusted computing base within the first host; and

requesting an authenticated infestation scan by trusted software.

Ex.1002
NETSKOPE, INC. / Page 342 of 378

12. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating is being performed.

13. A system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

14. A computer program product for protecting a network, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network;

quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

15. A method for processing requests from a quarantined host to communicate via a protected network, comprising:

receiving a service request sent by the quarantined host;

serving a quarantine notification page to the quarantined host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

16. A method as recited in claim 15, further comprising, in the event the service request comprises a DNS query, proxying the service request to a DNS service if the host name that is the subject of the DNS query is associated with a remediation host.

17. A method as recited in claim 15, wherein providing in response an IP address of a quarantine server includes providing a response with a short time to live.

Ex.1002
NETSKOPE, INC. / Page 343 of 378

18. A method for remedying an insecure condition in a host associated with a protected network, comprising:

detecting an open backdoor port on the host; and

using the open backdoor port to communicate with the host as required to remedy the insecure condition.

19. A method as recited in claim 18, further comprising determining that communication cannot be established with the host using a primary communication method.

20. A method as recited in claim 18, wherein detecting an open backdoor port on the host includes scanning the host for any open backdoor port.

Ex.1002
NETSKOPE, INC. / Page 344 of 378

CONTAGION ISOLATION AND INOCULATION

ABSTRACT OF THE DISCLOSURE

[0061] Contagion isolation and inoculation is disclosed. In some embodiments, a request is received from a host, e.g., via a network interface, to connect to a protected network. It is determined whether the host is required to be quarantined. If the host is required to be quarantined, the host is provided only limited access to the protected network. In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed. In various embodiments attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user.

Ex.1002
NETSKOPE, INC. / Page 345 of 378

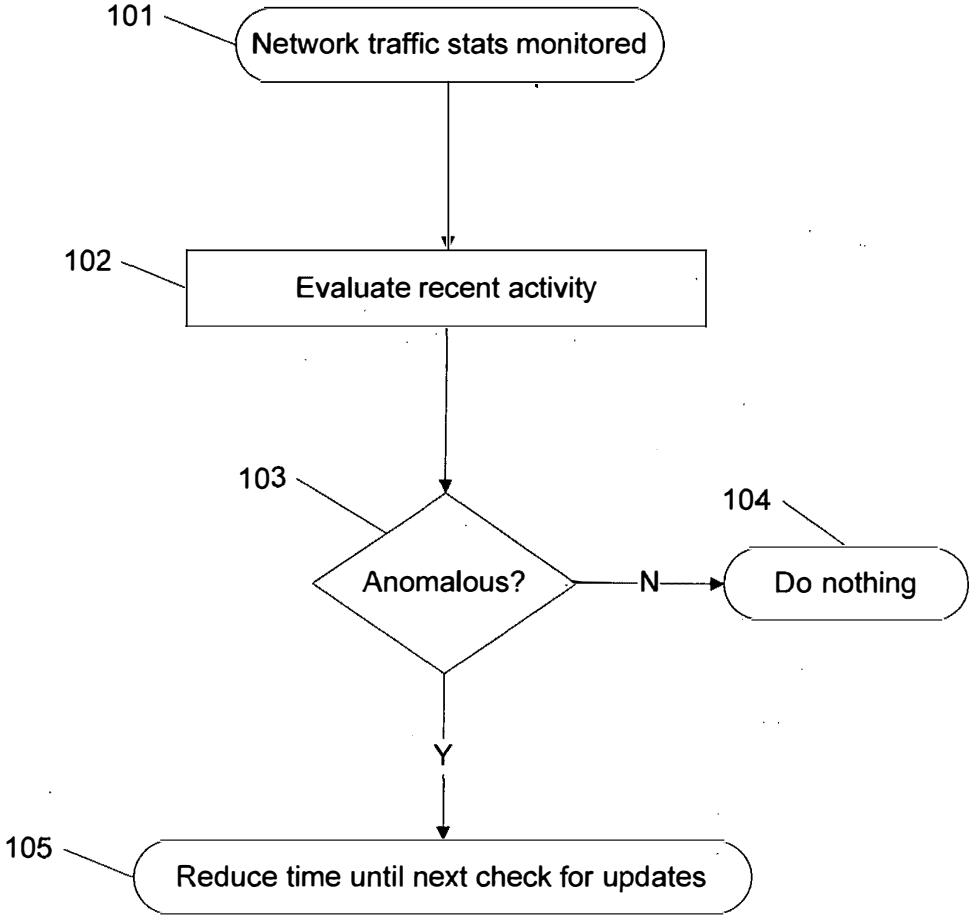


Figure 1

BEST AVAILABLE COPY

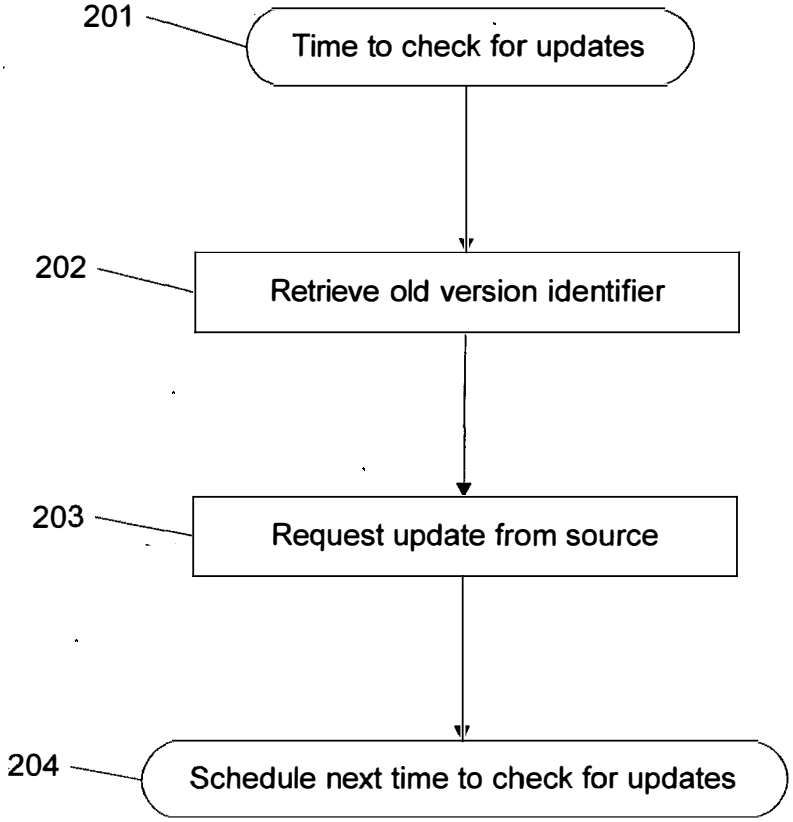

201
Time to check for updates
202
Retrieve old version identifier
203
Request update from source
204
Schedule next time to check for updates

Figure 2A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

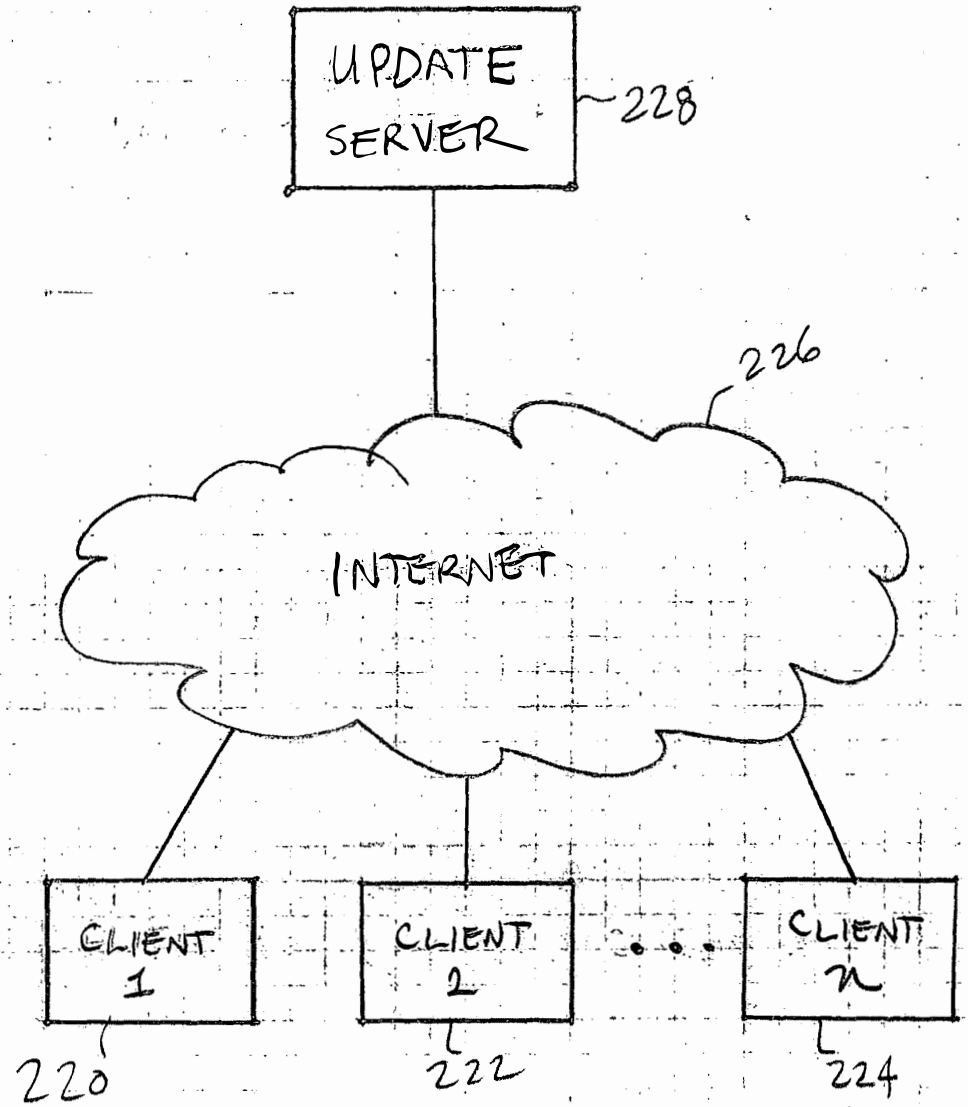


FIG. 2B

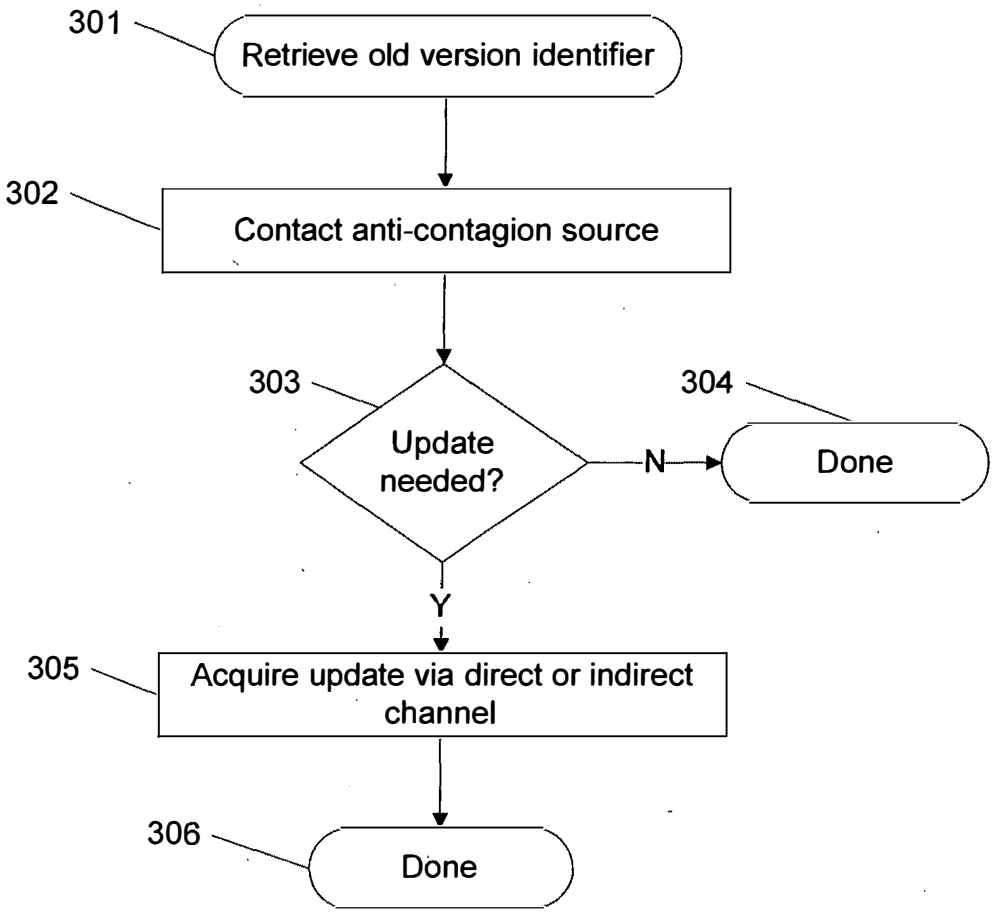

301
Retrieve old version identifier
302
Contact anti-contagion source
303
Update needed?
N
304
Done
Y
305
Acquire update via direct or indirect channel
306
Done

Figure 3A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

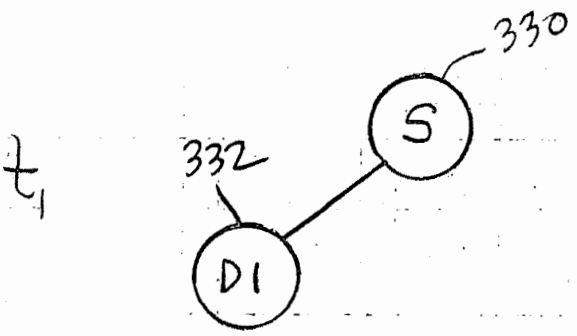


FIG. 3B

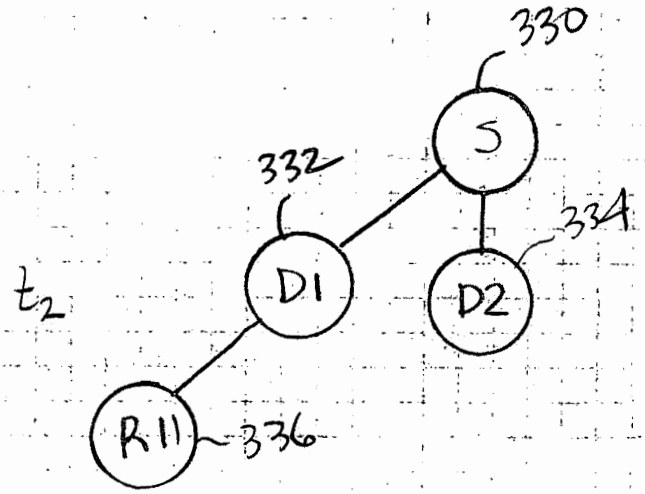


FIG. 3C

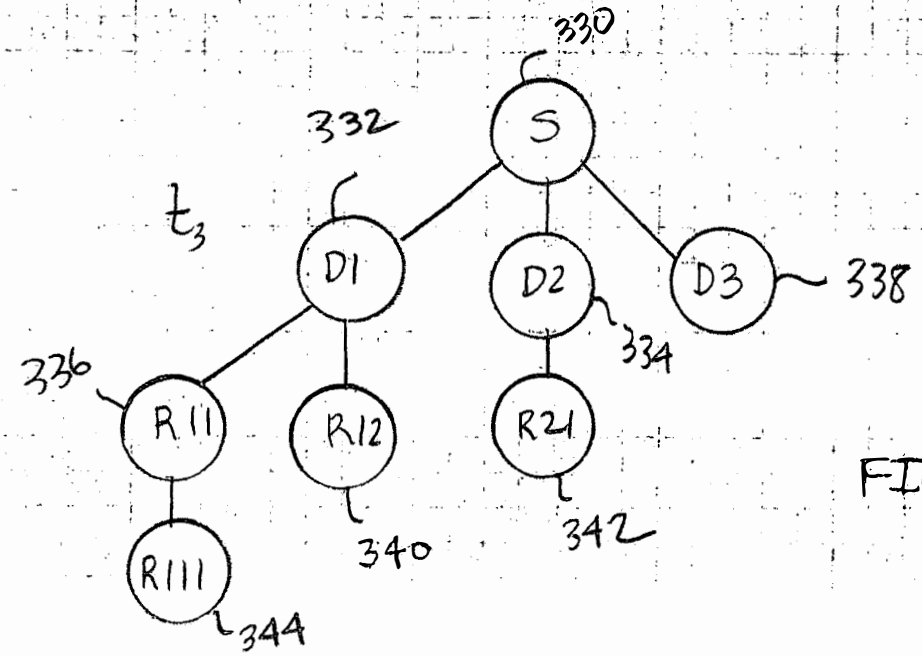


FIG. 3D

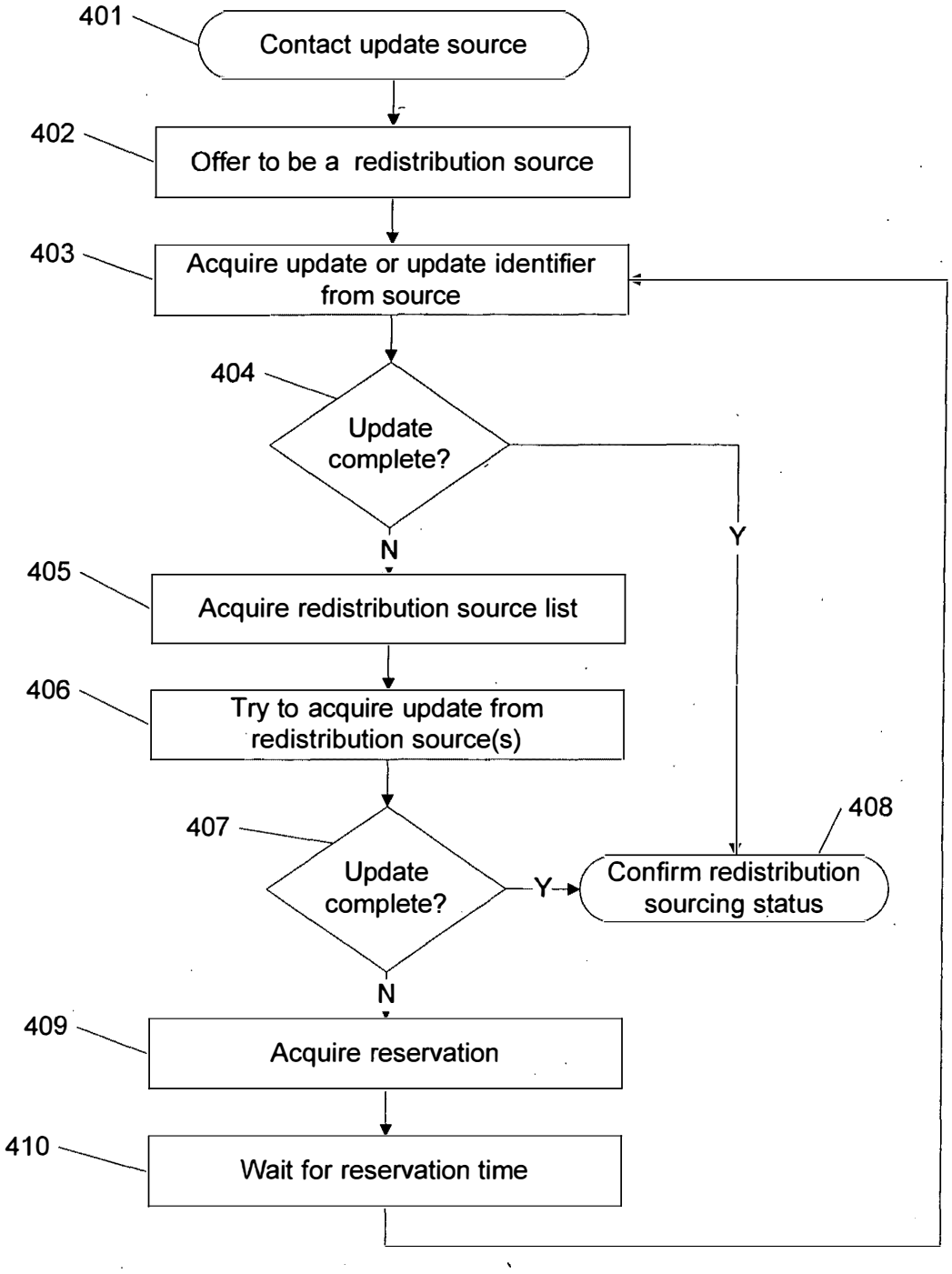

401
Contact update source
402
Offer to be a redistribution source
403
Acquire update or update identifier from source
404
Update complete?
N
Y
405
Acquire redistribution source list
406
Try to acquire update from redistribution source(s)
407
Update complete?
Y
408
Confirm redistribution sourcing status
N
409
Acquire reservation
410
Wait for reservation time

Figure 4A

STAEDTLER® No. 937 811E Engineer's Computation Pad

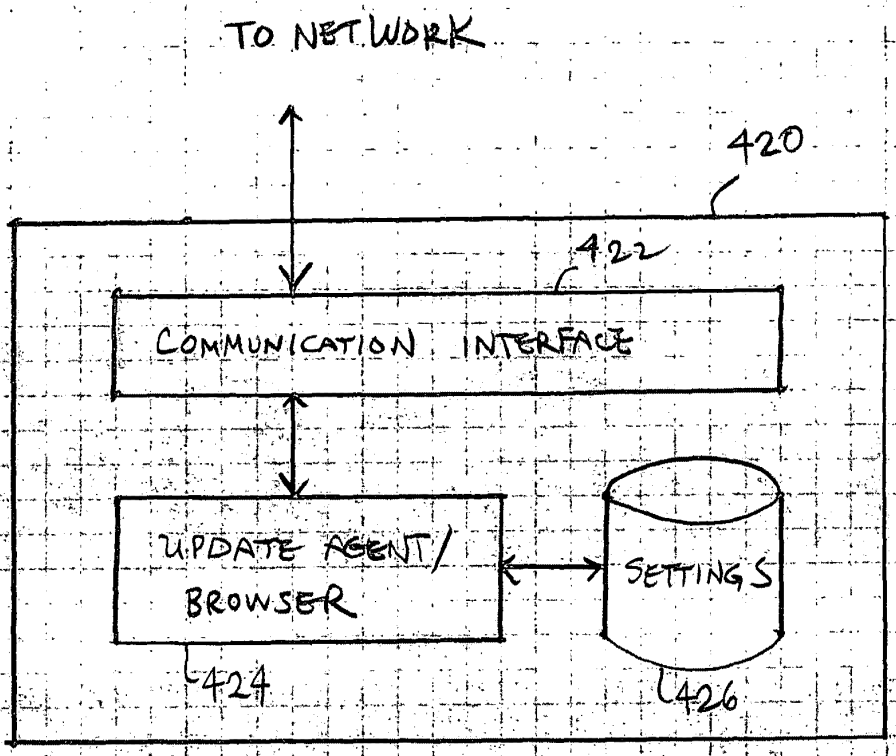


FIG. 4B

STAEDTLER® No. 937 811E
Engineer's Computation Pad

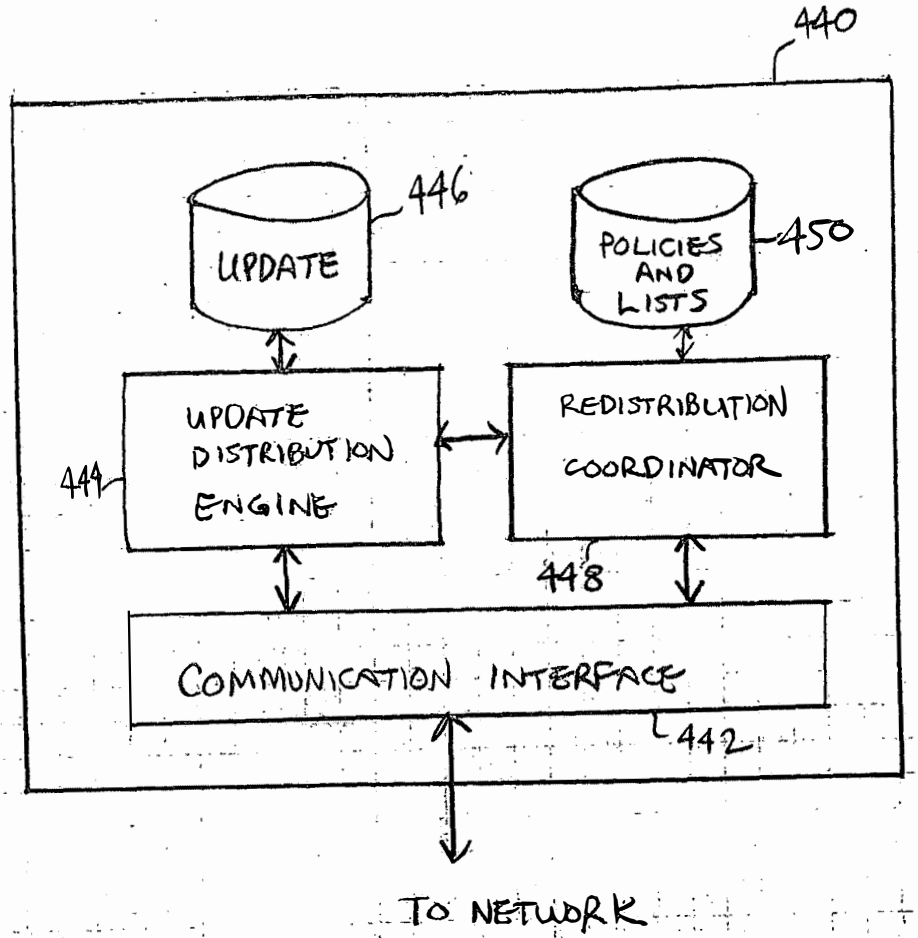


FIG. 4C

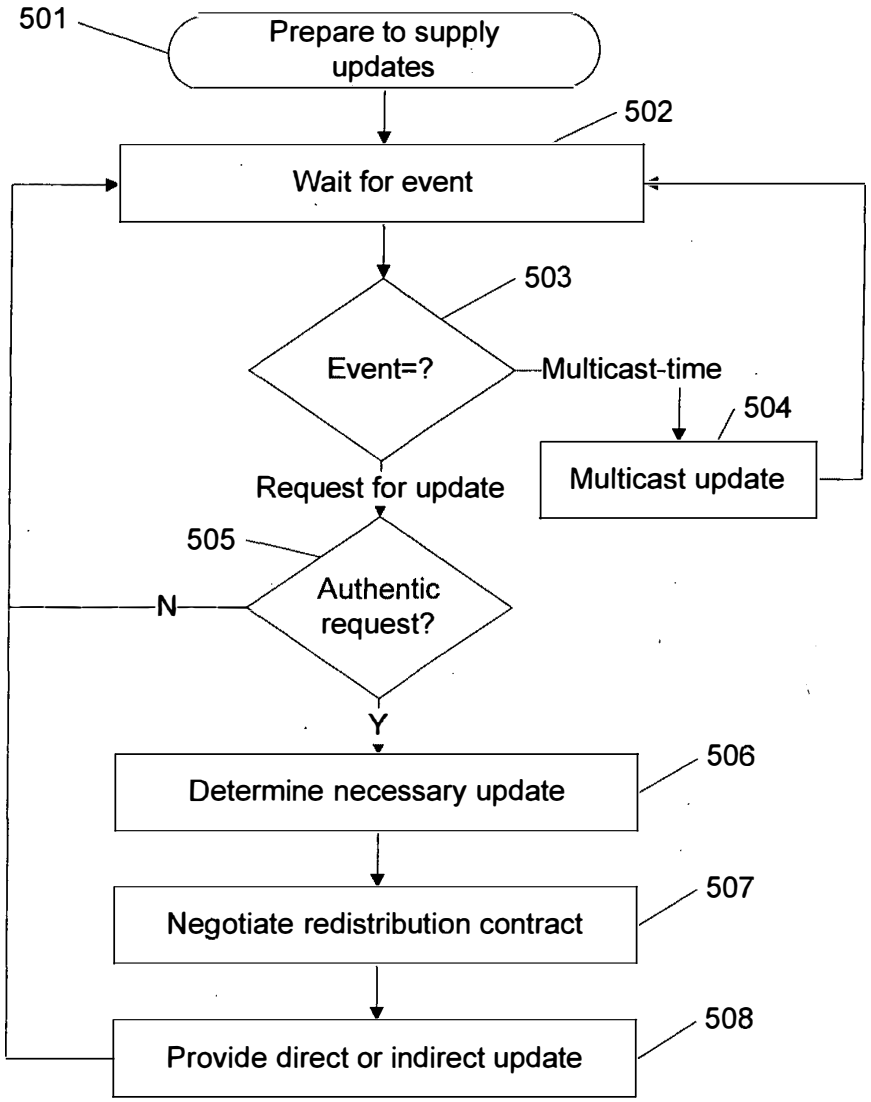

501
Prepare to supply updates
502
Wait for event
503
Event=?
Multicast-time
504
Multicast update
Request for update
505
Authentic request?
N
Y
506
Determine necessary update
507
Negotiate redistribution contract
508
Provide direct or indirect update

Figure 5

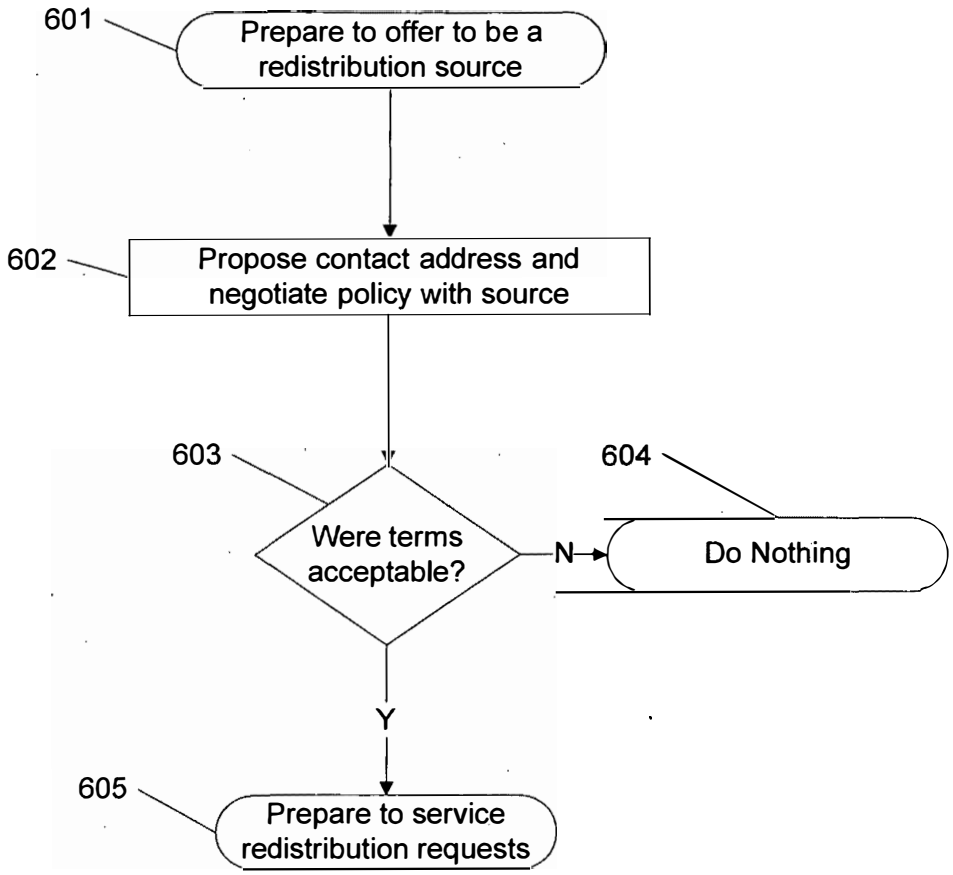

601
Prepare to offer to be a redistribution source
602
Propose contact address and negotiate policy with source
603
Were terms acceptable?
N
604
Do Nothing
Y
605
Prepare to service redistribution requests

Figure 6

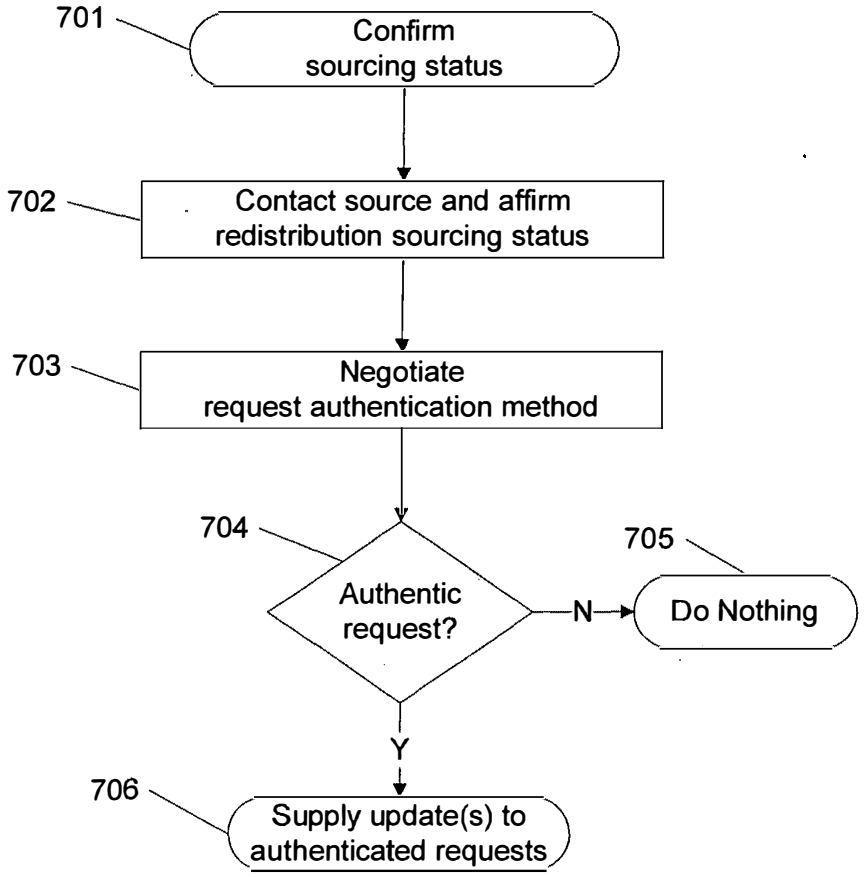

701
Confirm sourcing status
702
Contact source and affirm redistribution sourcing status
703
Negotiate request authentication method
704
Authentic request?
N
705
Do Nothing
Y
706
Supply update(s) to authenticated requests

Figure 7

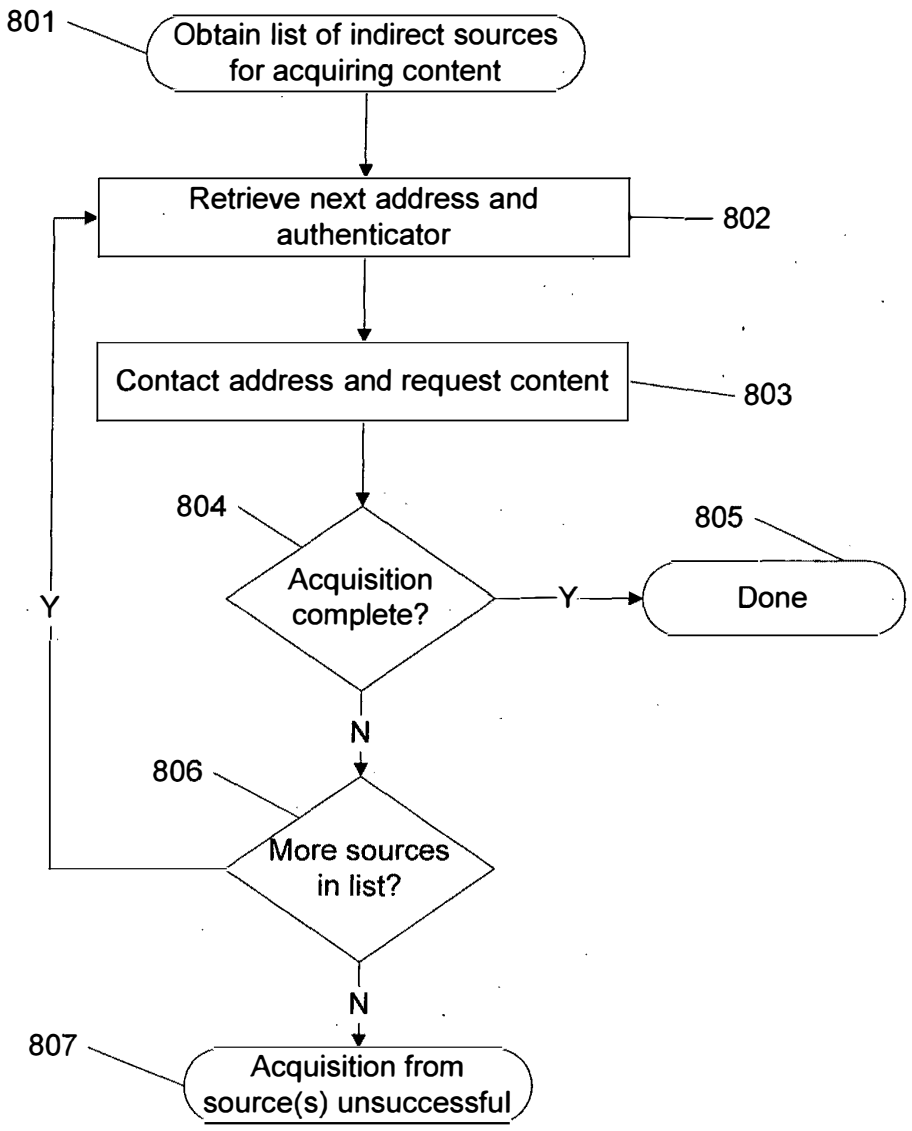

801
Obtain list of indirect sources for acquiring content
Retrieve next address and authenticator
802
Contact address and request content
803
804
Acquisition complete?
Y
805
Done
Y
N
806
More sources in list?
Y
N
807
Acquisition from source(s) unsuccessful

Figure 8

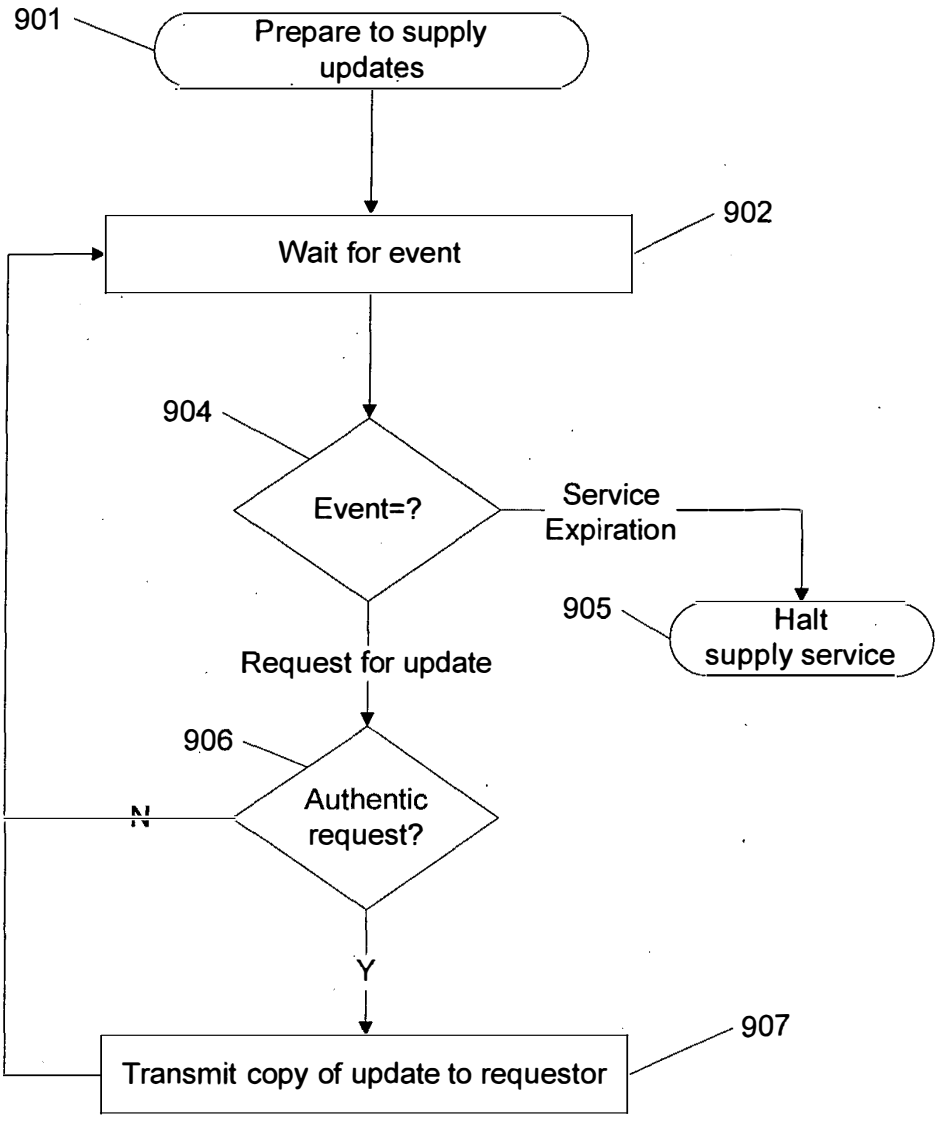

901
Prepare to supply updates
902
Wait for event
904
Event=?
Service Expiration
905
Halt supply service
Request for update
906
Authentic request?
N
Y
907
Transmit copy of update to requestor

Figure 9

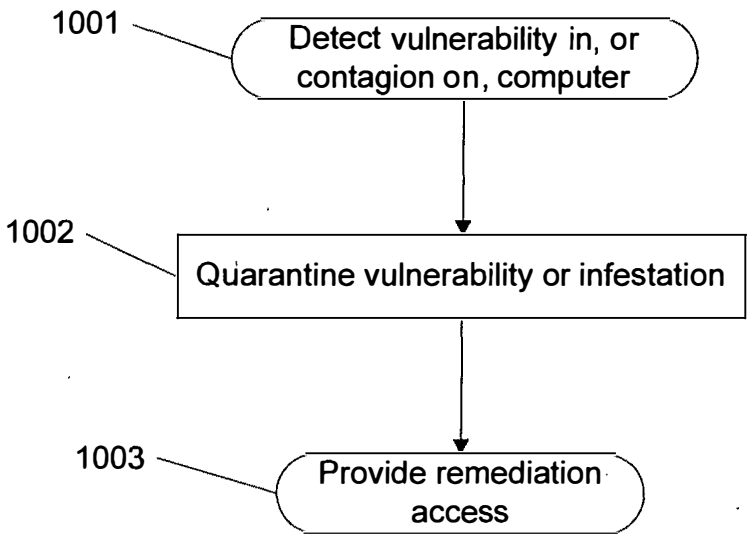

1001
Detect vulnerability in, or contagion on, computer
1002
Quarantine vulnerability or infestation
1003
Provide remediation access

Figure 10A

STAEDTLER® No. 937 811E Engineer's Computation Pad

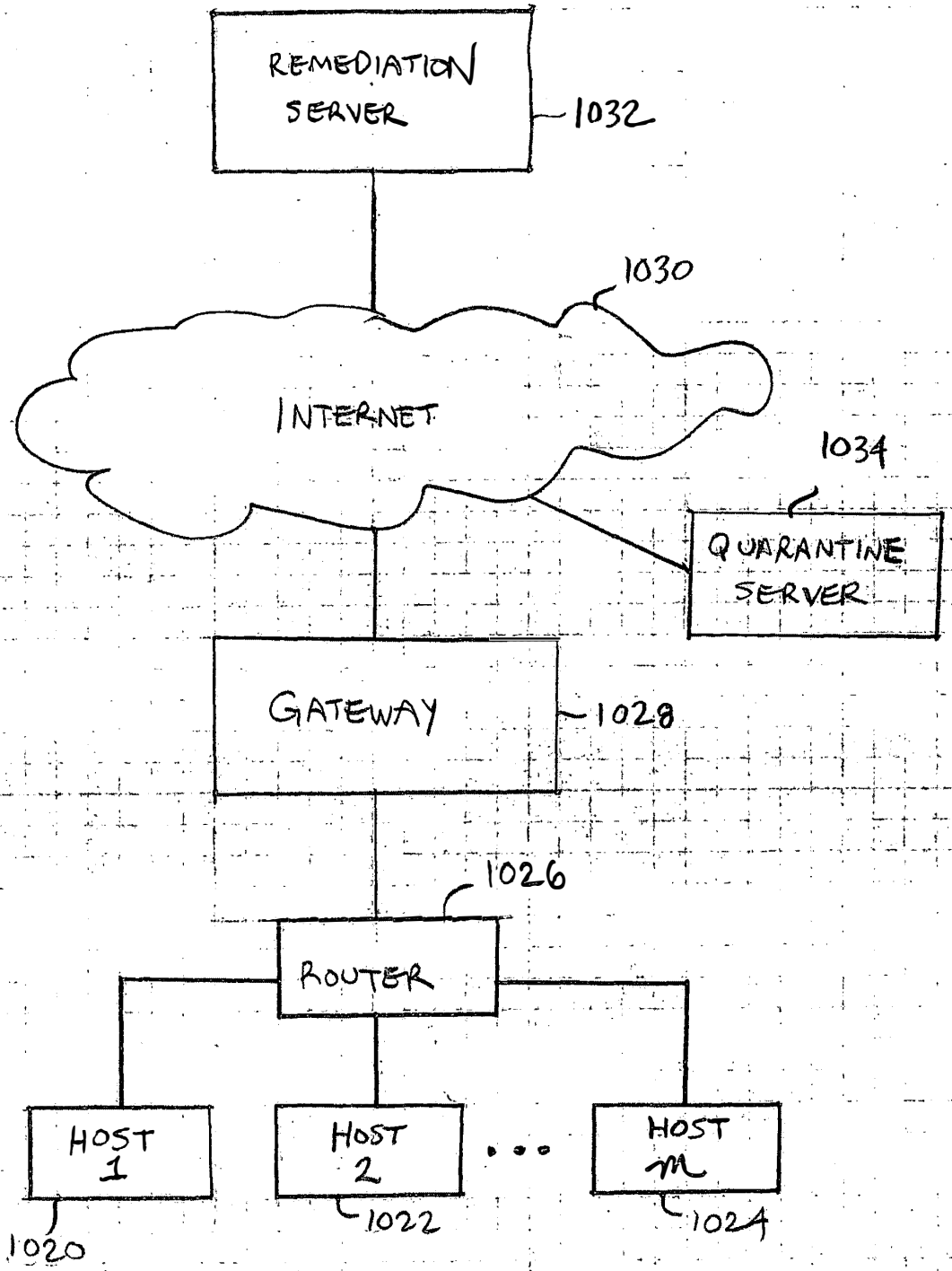


FIG. 10B

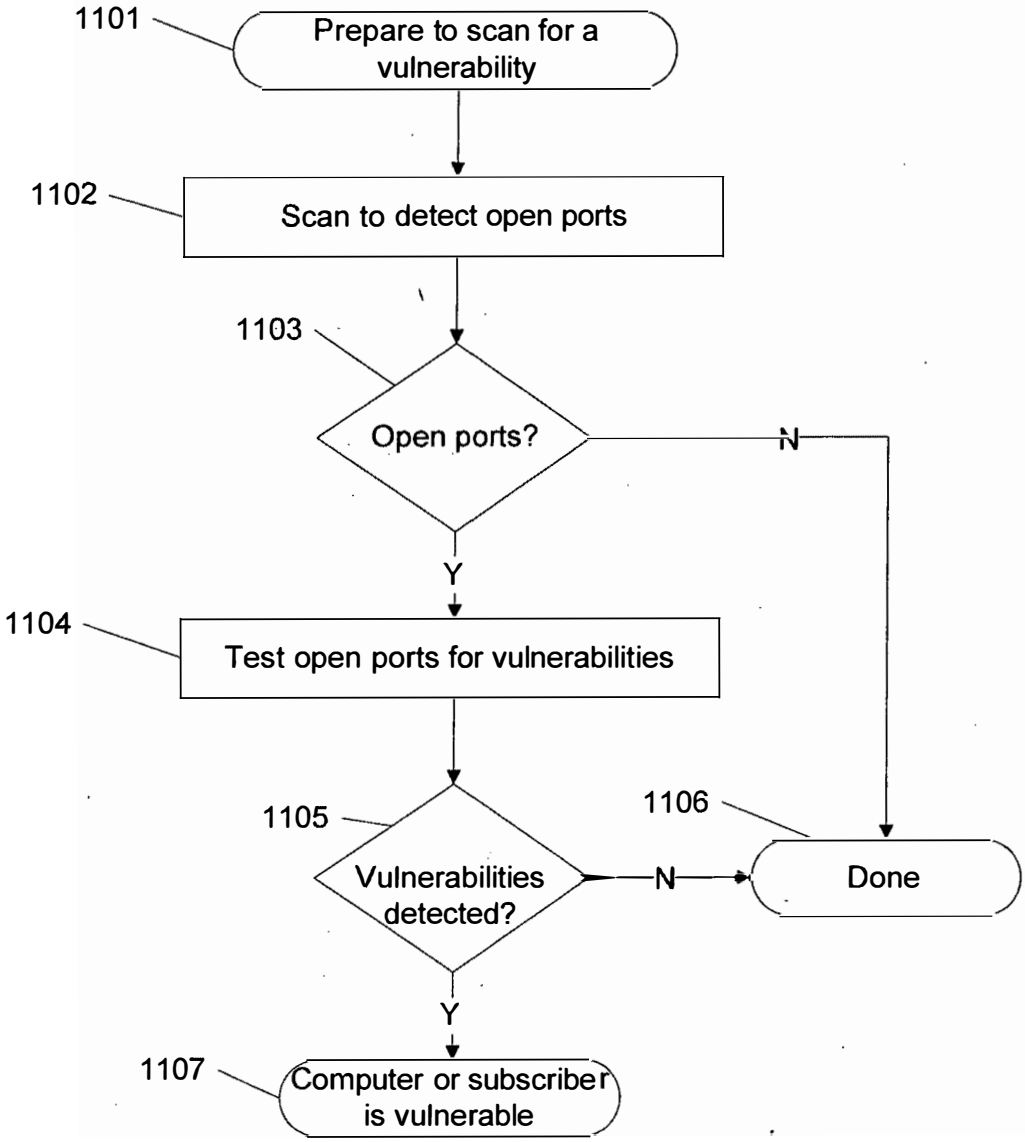

1101
Prepare to scan for a vulnerability
1102
Scan to detect open ports
1103
Open ports?
N
Y
1104
Test open ports for vulnerabilities
1105
Vulnerabilities detected?
1106
N
Done
Y
1107
Computer or subscriber is vulnerable

Figure 11

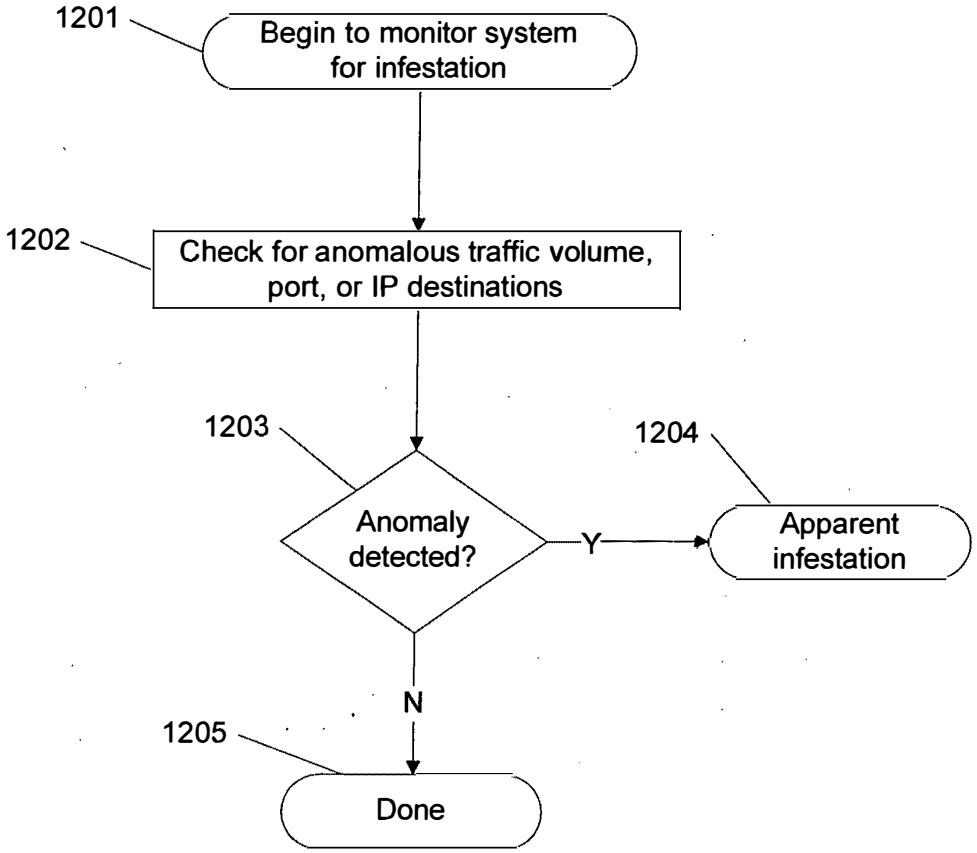

1201
Begin to monitor system for infestation
1202
Check for anomalous traffic volume, port, or IP destinations
1203
Anomaly detected?
Y
1204
Apparent infestation
N
1205
Done

Figure 12

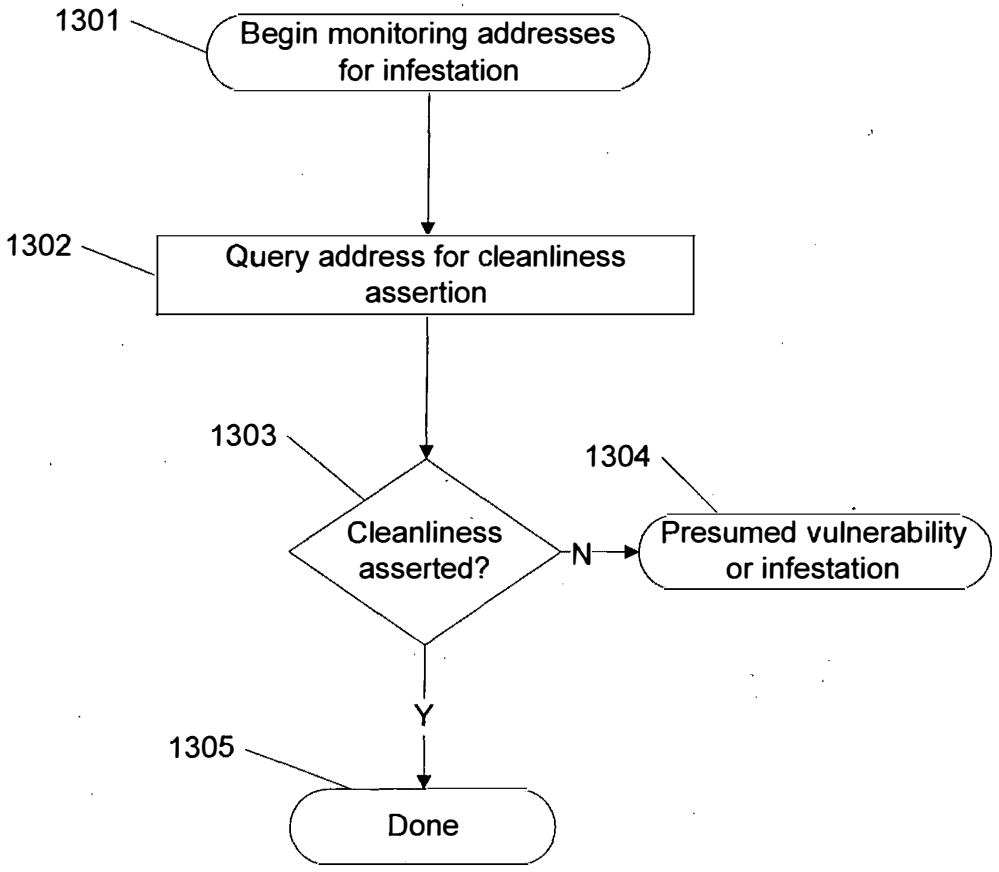

1301
Begin monitoring addresses for infestation
1302
Query address for cleanliness assertion
1303
Cleanliness asserted?
N
1304
Presumed vulnerability or infestation
Y
1305
Done

Figure 13

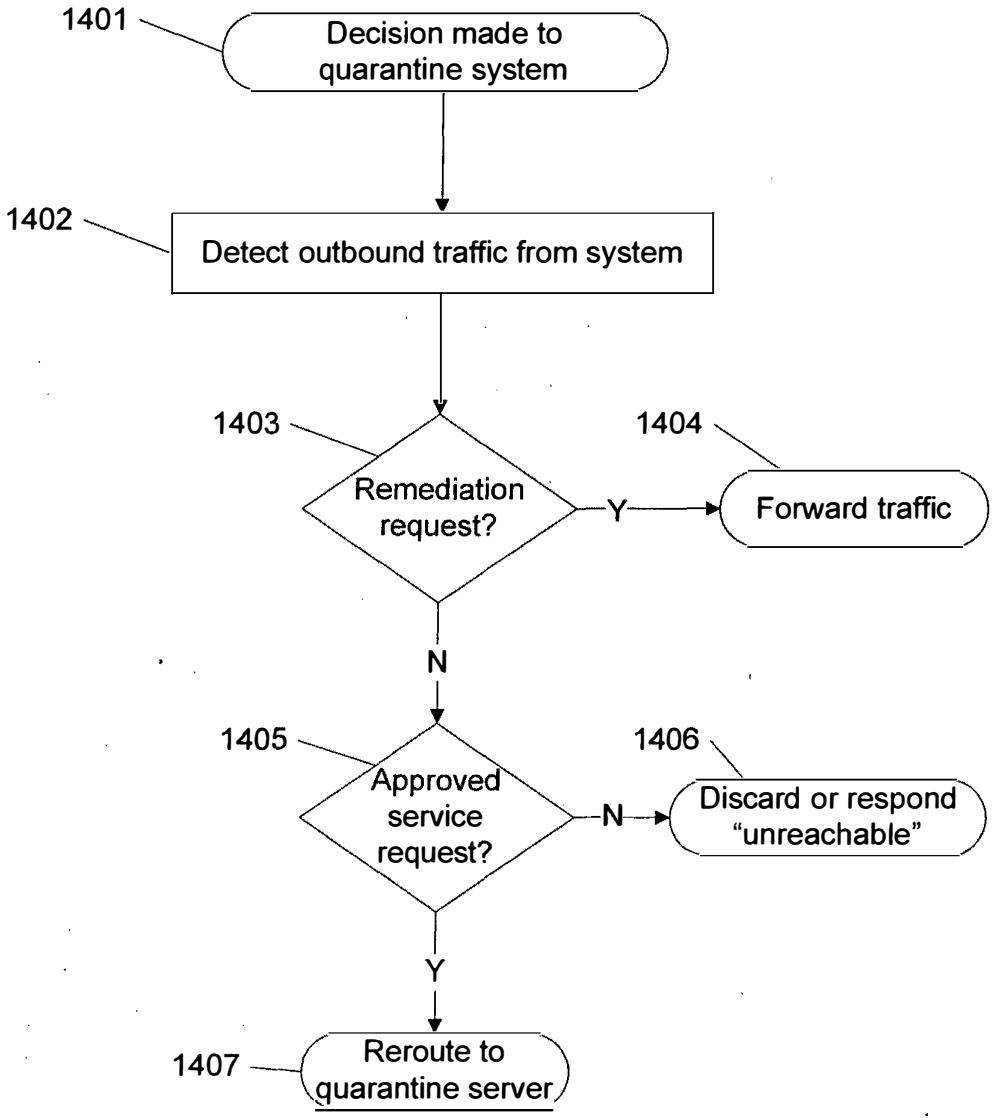

1401
Decision made to quarantine system
1402
Detect outbound traffic from system
1403
Remediation request?
Y
1404
Forward traffic
N
1405
Approved service request?
N
1406
Discard or respond "unreachable"
Y
1407
Reroute to quarantine server

Figure 14

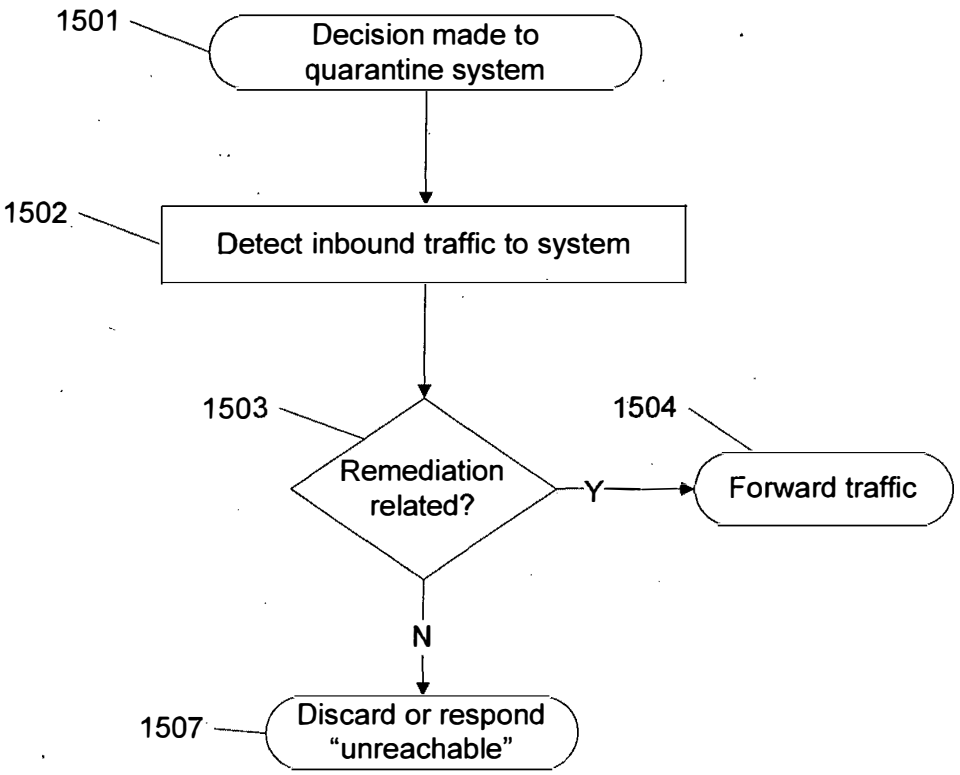

1501
Decision made to quarantine system
1502
Detect inbound traffic to system
1503
Remediation related?
Y
1504
Forward traffic
N
1507
Discard or respond "unreachable"

Figure 15

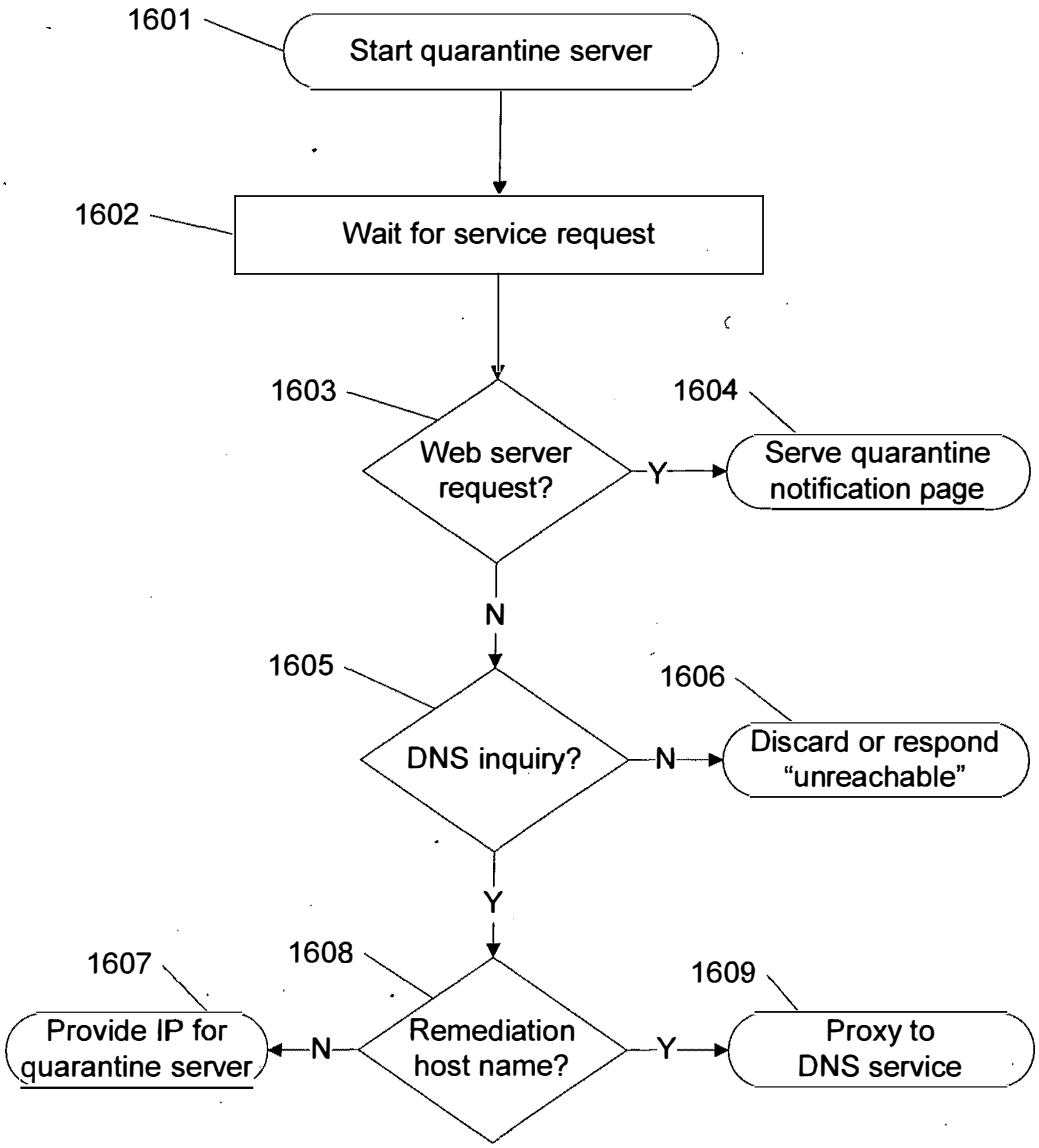

1601
Start quarantine server
1602
Wait for service request
1603
Web server request?
Y
1604
Serve quarantine notification page
N
1605
DNS inquiry?
N
1606
Discard or respond "unreachable"
Y
1607
Provide IP for quarantine server
N
1608
Remediation host name?
Y
1609
Proxy to DNS service

Figure 16

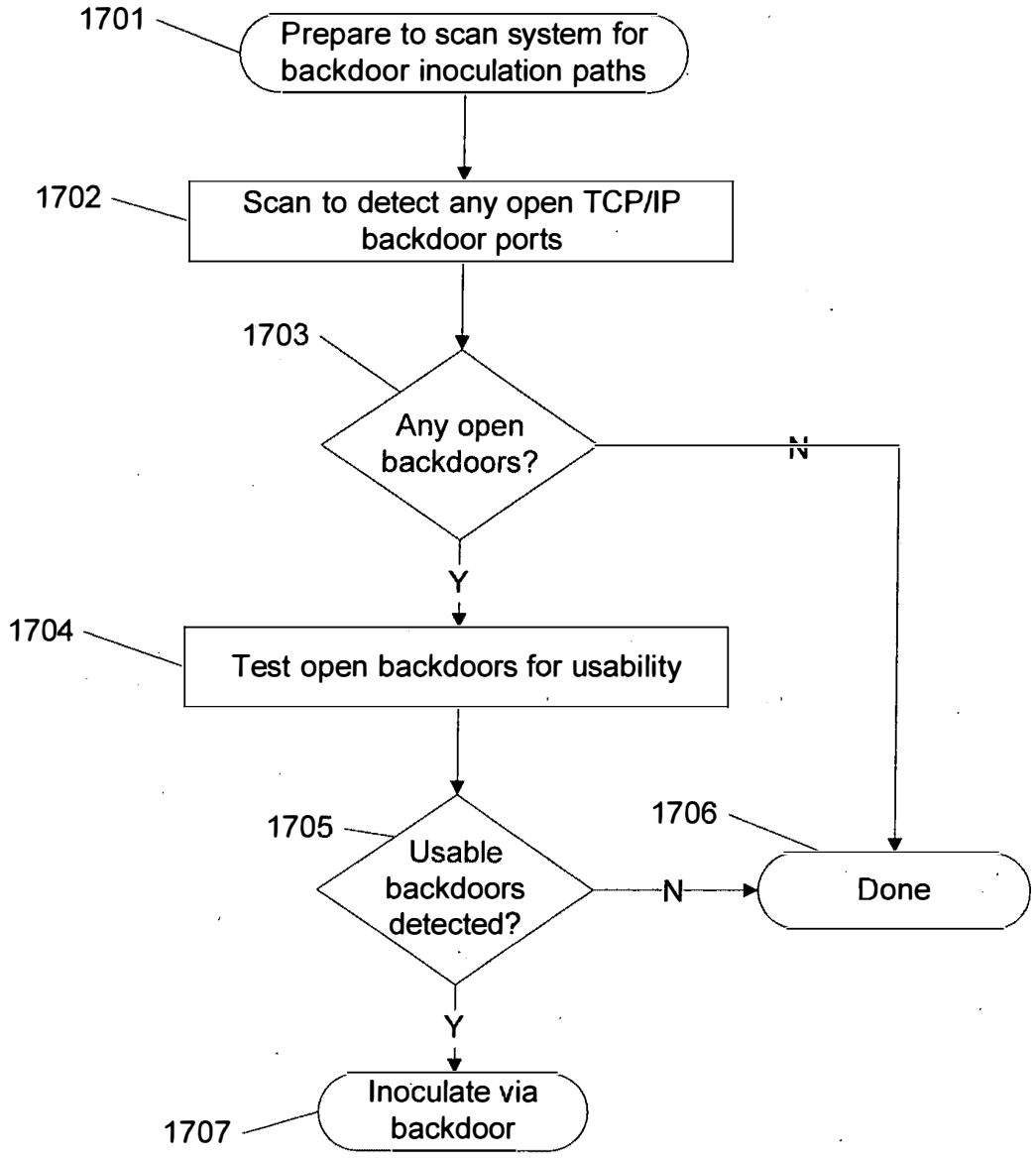

1701
Prepare to scan system for backdoor inoculation paths
1702
Scan to detect any open TCP/IP backdoor ports
1703
Any open backdoors?
N
Y
1704
Test open backdoors for usability
1705
Usable backdoors detected?
N
1706
Done
Y
Inoculate via backdoor
1707

Figure 17

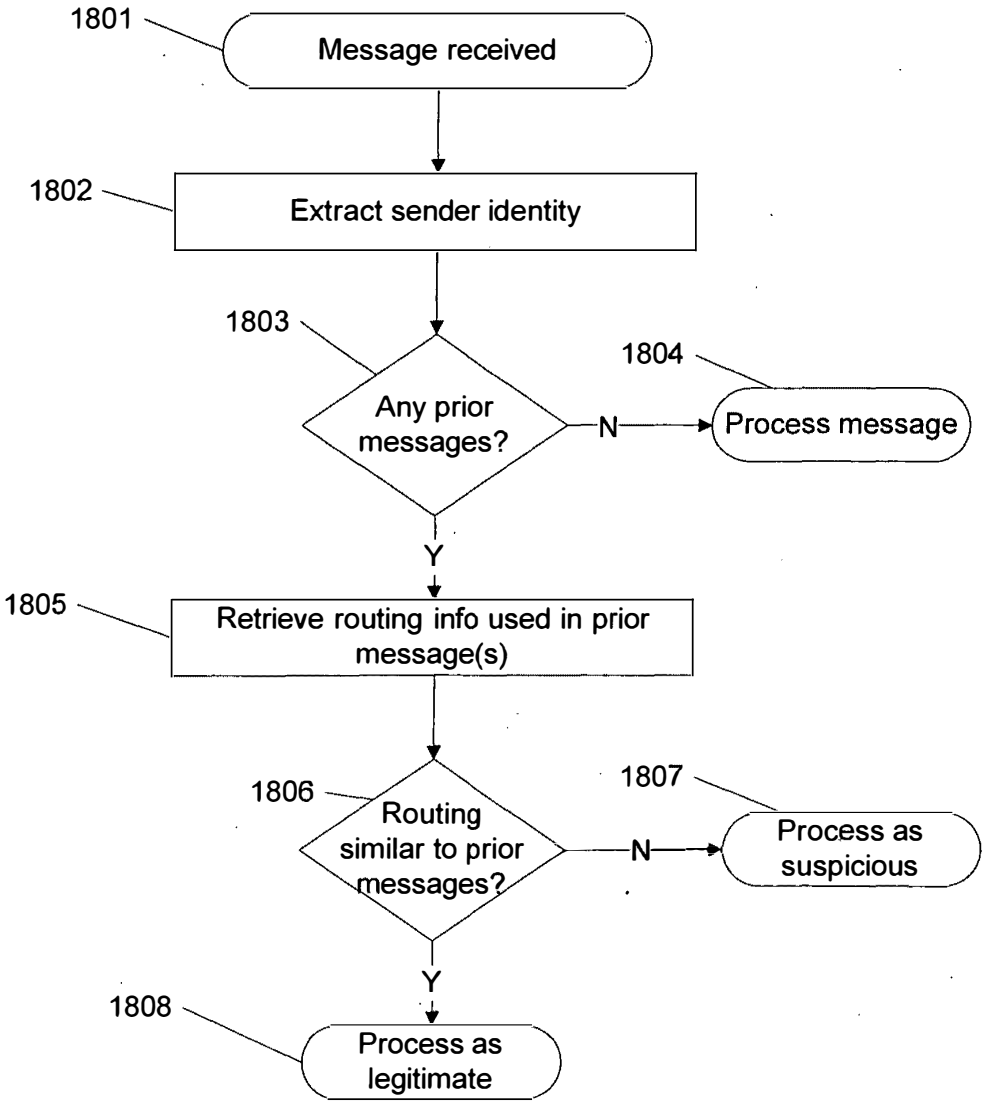

1801
Message received
1802
Extract sender identity
1803
Any prior messages?
N
1804
Process message
Y
1805
Retrieve routing info used in prior message(s)
1806
Routing similar to prior messages?
N
1807
Process as suspicious
Y
1808
Process as legitimate

Figure 18

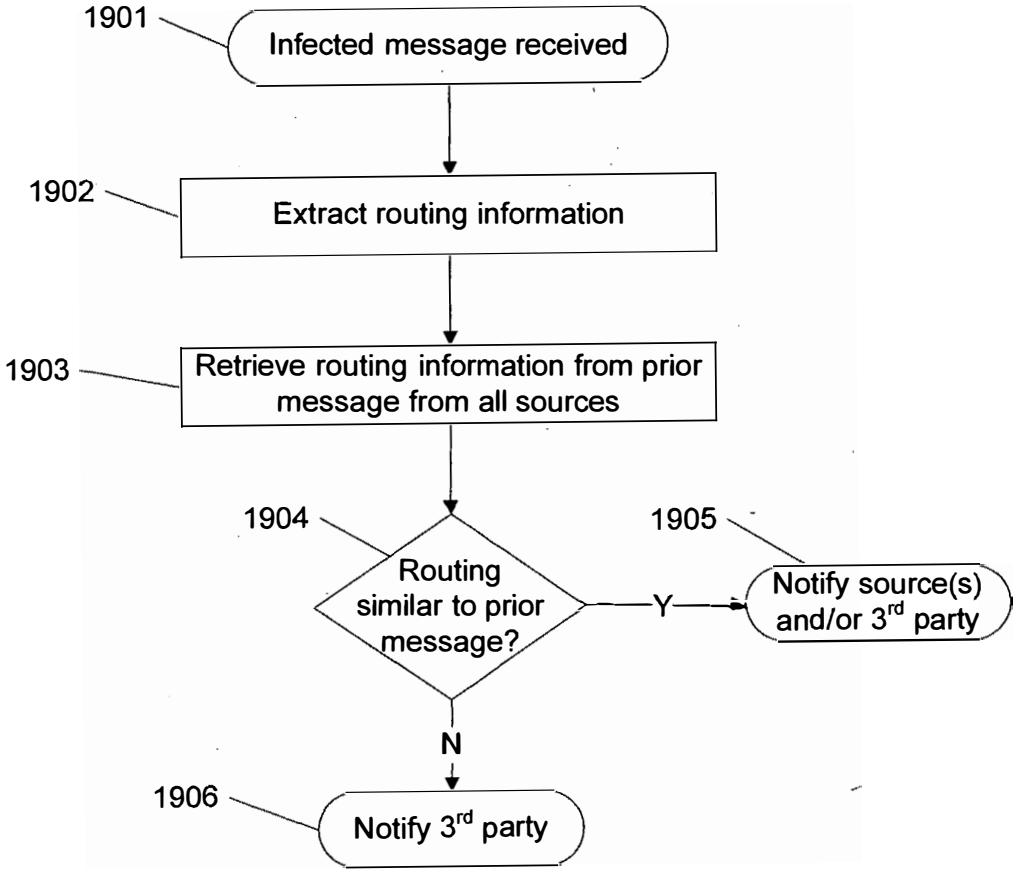

1901
Infected message received
1902
Extract routing information
1903
Retrieve routing information from prior message from all sources
1904
Routing similar to prior message?
Y
1905
Notify source(s) and/or 3rd party
N
1906
Notify 3rd party

Figure 19A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

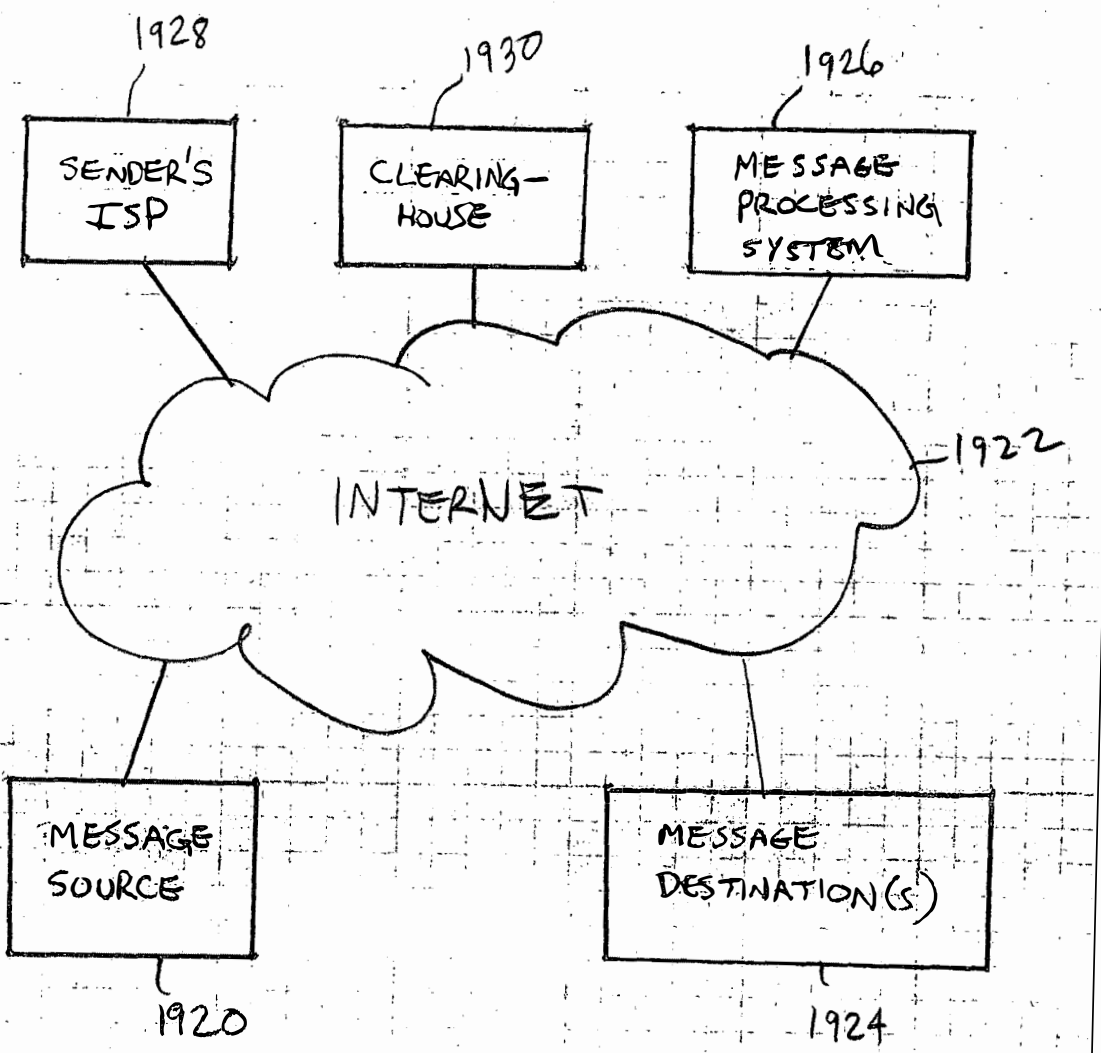


FIG. 19B

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

DECLARATION AND POWER OF ATTORNEY FOR ORIGINAL U.S. PATENT APPLICATION

Attorney's Docket No. RAD2P001

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **CONTAGION ISOLATION AND INOCULATION**, the specification of which,

(check one)

1. ☒ is attached hereto.

2. ☐ was filed on _____ as
U.S. Application No. _____
and was amended on _____.

3. ☐ was filed on _____ as
International PCT Application No. _____
and was amended on _____.

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.

For Assigned Inventions: I understand that the purpose of making this appointment is to permit prosecution of patent applications for the above-identified invention for the benefit of my assignee, and that this appointment does not create an attorney-client relationship between me and these appointees.

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

I hereby claim foreign priority benefits under Title 35, United States code, § 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, listed below and have identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Benefits Claimed?
_____	_____	_____	☐Yes ☐No
(Appl. No.)	(Country)	(Filing Date)	

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

Prior Provisional Application(s)

60/613,909	09/27/2004
(Application No.)	(Filing Date)

BEST AVAILABLE COPY

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, 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 Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Application(s)

(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)

And I hereby appoint the law firm of Van Pelt, Yi & James LLP, including **Lee Van Pelt (Reg. No. 38,352); Susan C. Yi (Reg. No. 39,883); and William J. James (Reg. No. 40,661) Diana Y. Fu (Reg. No. 52,924) and Clover Huang (Reg. No. 55,285)** as my principal attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Please Direct all Correspondence To: **Customer No. 21912**
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

Direct Telephone Calls To: **William J. James at telephone number (408) 973-2592**

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 issuing thereon.

Full name of sole or first inventor	James A. Roskind				
Signature of sole or first inventor				Date:	Sept 27, 2005
Residence: City	Redwood City	State:	CA	Citizenship:	United States of America
Mailing Address	920 Governors Bay Drive, Redwood City, CA 94065				

Full name of second inventor	Aaron T. Emigh				
Signature of second inventor				Date:	_____, 2005
Residence: City	Incline Village	State:	NV	Citizenship:	United States of America
Mailing Address	762 Judith Court, Incline Village, NV 89451				

BEST AVAILABLE COPY

DECLARATION AND POWER OF ATTORNEY FOR ORIGINAL U.S. PATENT APPLICATION

Attorney's Docket No. RAD2P001

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **CONTAGION ISOLATION AND INOCULATION**, the specification of which,

(check one)

1. ☒ is attached hereto.

2. ☐ was filed on _____ as U.S. Application No. _____ and was amended on _____.

3. ☐ was filed on _____ as International PCT Application No. _____ and was amended on _____.

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.

For Assigned Inventions: I understand that the purpose of making this appointment is to permit prosecution of patent applications for the above-identified invention for the benefit of my assignee, and that this appointment does not create an attorney-client relationship between me and these appointees.

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

I hereby claim foreign priority benefits under Title 35, United States code, § 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, listed below and have identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Benefits Claimed?
_____	_____	_____	☐Yes ☐No
(Appl. No.)	(Country)	(Filing Date)	

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

Prior Provisional Application(s)

60/613,909	09/27/2004
(Application No.)	(Filing Date)

BEST AVAILABLE COPY

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, 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 Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Application(s)

(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)

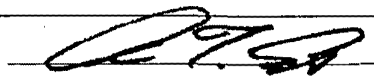
And I hereby appoint the law firm of Van Pelt, Yi & James LLP, including **Lee Van Pelt (Reg. No. 38,352); Susan C. Yi (Reg. No. 39,883); and William J. James (Reg. No. 40,661) Diana Y. Fu (Reg. No. 52,924) and Clover Huang (Reg. No. 55,285)** as my principal attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Please Direct all Correspondence To: **Customer No. 21912**
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

Direct Telephone Calls To: **William J. James at telephone number (408) 973-2592**

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 issuing thereon.

Full name of sole or first inventor	James A. Roskind				
Signature of sole or first inventor	_____			Date:	_____, 2005
Residence: City	Redwood City	State:	CA	Citizenship:	United States of America
Mailing Address	920 Governors Bay Drive, Redwood City, CA 94065				

Full name of second inventor	Aaron T. Emigh				
Signature of second inventor				Date:	September 27, 2005
Residence: City	Incline Village	State:	NV	Citizenship:	United States of America
Mailing Address	762 Judith Court, Incline Village, NV 89451				

BEST AVAILABLE COPY

PATENT APPLICATION SERIAL NO _____

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

09/30/2005 FFANAIA2 00000018 11237003

01 FC:2011	150.00	OP
02 FC:2111	250.00	OP
03 FC:2311	100.00	OP
04 FC:2201	200.00	OP

PTO-1556
(5/87)

U.S. Government Printing Office: 2002 — 466-267/69033

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number: 112377003

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150.00		N/A	300.00
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	$250		N/A	$500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	$100		N/A	$200
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	-	X$ 25 =		OR	X$50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	5 minus 3 =	2	X100 =	200		X200 =	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			+180=			+360=	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	700		TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT A	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

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.

PTO/SB/35 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U. S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)

First Named Inventor	James A. Roskind
Title	CONTAGION ISOLATION AND INOCULATION
Attorney Docket Number	RAD2P001

I hereby 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 agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).

William J. James — Signature

9/27/05 — Date

William J. James — Typed or printed name

40,661 — Registration Number, if applicable

408-973-2585 — Telephone Number

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing.**

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 122(b)(2)(B)(iii)).**

This collection of information is required by 37 CFR 1.213(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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