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

GOOGLE EXHIBIT 1003
Google v. K.Mizra
IPR2025-01437

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

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

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.]

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

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
FEDFF3D4B86A46C...
Name: Bradley Sharp
Title: Receiver

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

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		
	8,965,892		
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		
	8,180,687		
	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	
	8,539,107		
	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.

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

DocuSign Envelope ID: FC81257A-F6D0-4296-89B4-7D6A643A611E

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.

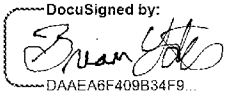
This Assignment shall be binding upon and shall inure to the benefit of the parties and their respective successors and assigns.

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

DocuSign Envelope ID: FC81257A-F6D0-4296-89B4-7D6A643A611E

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
11/237,004	09/27/2005	James A. Roskind	GLIA -030US-2

CONFIRMATION NO. 6024

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

POA ACCEPTANCE LETTER

OC000000101709915

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
11/237,004	09/27/2005	James A. Roskind	PB-036

CONFIRMATION NO. 6024

POWER OF ATTORNEY NOTICE

85853
Aaron Emigh
762 Judith Court
Incline Village, NV 89451

OC000000101709867

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/

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	11/237,004
Filing Date	9-27-2005
First Named Inventor	James A. Roskind
Title	Detecting and processing suspicious network communications
Art Unit	2476
Examiner Name	WEIDNER, TIMOTHY J
Attorney Docket Number	GLIA-030US-2

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.: 11/237,004 Filed/Issue Date: 09-27-2005

Titled: Detecting and processing suspicious network communications

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 0422, 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 0092, 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

[Page 2 of 2]

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:	33429153
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Joseph John Basista
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	09-AUG-2018
Filing Date:	27-SEP-2005
Time Stamp:	19:54:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	GLIA-030US-2-Form82A-aia0082.pdf	174295 f366f83aea19a7629c9e3e2a60ed188db8145ead	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-2-373Statement-aia0096.pdf	122737 52105c69e2e5b4941901f6c1d0c5d65c046c9a85	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	441005	

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,004	07/19/2016	9398037	PB-036	6024

85853 7590 06/29/2016

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 749 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 04/27/2016

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 Emigh	(Depositor's name)
/ Aaron T. Emigh /	(Signature)
June 20, 2016	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

TITLE OF INVENTION: Detecting and processing suspicious network communications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/27/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
WEIDNER, TIMOTHY J	2476	370-401000

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, NV

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

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

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

☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 50-4831 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature / Aaron T. Emigh / Date June 20, 2016

Typed or printed name Aaron Emigh Registration No. _____

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

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	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt

EFS ID:	26120737
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	20-JUN-2016
Filing Date:	27-SEP-2005
Time Stamp:	21:23:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	6811
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 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 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-036-issue-fee.pdf	234547 86b873faf53358bb759baf9e9f833b4e51b5ecd1	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30177 56c3a4a65b68a5caeb110c8765b98960a7218a11	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	264724		

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

85853 7590 04/27/2016

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER
WEIDNER, TIMOTHY J

ART UNIT	PAPER NUMBER
2476	

DATE MAILED: 04/27/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

TITLE OF INVENTION: Detecting and processing suspicious network communications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/27/2016

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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

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

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **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 04/27/2016

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

TITLE OF INVENTION: Detecting and processing suspicious network communications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/27/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
WEIDNER, TIMOTHY J	2476	370-401000

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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 04/27/2016

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	

ART UNIT	PAPER NUMBER
2476	

DATE MAILED: 04/27/2016

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND 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.

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.

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2476	

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

(1) *Timothy J. Weidner*. (3)_____.

(2) *Aaron Emigh (Applicant)*. (4)_____.

Date of Interview: *22 March 2016*.

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: *31,42 and 49*.

Identification of prior art discussed: *Olivier and Gleichauf*.

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...)

Amendment and Response on December 28, 2015 were presented and discussed. Applicant indicated the prior art does not describe or suggest the present claimed subject matter, as shown in the amendment and response. Examiner indicated agreement for the above matters. In view of the above, the present claimed subject matter is considered to be allowable subject matter.

Applicant recordation instructions: 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

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

/Timothy J Weidner/ Primary Examiner, Art Unit 2476	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Notice of Allowability	Application No. 11/237,004	Applicant(s) ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2476	AIA (First Inventor to File) Status No

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment and Response on December 28, 2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *31,34-42,45-49 and 52-54 (Renumbered 1-18)*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *Mar. 22, 2016* .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Timothy J Weidner/
Primary Examiner, Art Unit 2476

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2476	

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

(1) *Timothy J. Weidner*. (3)_____.

(2) *Aaron Emigh (Applicant)*. (4)_____.

Date of Interview: *22 March 2016*.

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: *31,42 and 49*.

Identification of prior art discussed: *Olivier and Gleichauf*.

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...)

Amendment and Response on December 28, 2015 were presented and discussed. Applicant indicated the prior art does not describe or suggest the present claimed subject matter, as shown in the amendment and response. Examiner indicated agreement for the above matters. In view of the above, the present claimed subject matter is considered to be allowable subject matter.

Applicant recordation instructions: 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

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

/Timothy J Weidner/ Primary Examiner, Art Unit 2476	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J Weidner	2476

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
eDAN inventorship search	9/25/2008	TJW
EAST search class/sub 370/252,389,401 713/153,154 726/22,26,27 using keywords	9/29/2008	TJW
eDAN and EAST searches above updated	7/7/2009	TJW
EAST keyword search	7/7/2009	TJW
eDAN and EAST searches above updated	5/28/2010	TJW
EAST keyword search	5/28/2010	TJW
eDAN and EAST searches above updated	2/15/2011	TJW
EAST keyword search	2/15/2011	TJW
USPAT and US-PGPUB search using limited classification	6/18/2015	TJW
Updated previous searches	3/22/2016	TJW

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	Interference search of record	3/22/2016	TJW

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1621	IP with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	USPAT	OR	OFF	2016/03/22 10:20
S2	871	IP adj address$5 with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	USPAT	OR	OFF	2016/03/22 10:20
S3	573	S2 and (instant adj messag$5 email e?mail e adj mail)	USPAT	OR	OFF	2016/03/22 10:20
S4	194	S3 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	USPAT	OR	OFF	2016/03/22 10:20
S5	1645	IP adj address$5 same (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	USPAT	OR	OFF	2016/03/22 10:20
S6	538	S5 and geographic$5	USPAT	OR	OFF	2016/03/22 10:20
S7	164	S6 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	USPAT	OR	OFF	2016/03/22 10:20
S8	6818	(G06F21/55$ G06F21/56$ H04L29/06551 H04L29/06877-06918 H04L51/12 H04L51/20 H04L63/14-145).cpc.	USPAT	OR	OFF	2016/03/22 10:20
S9	2924	S8 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	USPAT	OR	OFF	2016/03/22 10:20
S10	838	S9 and IP adj address	USPAT	OR	OFF	2016/03/22 10:20
S11	575	S10 and match$5	USPAT	OR	OFF	2016/03/22 10:20
S12	164	S11 and IP adj address same match$5	USPAT	OR	OFF	2016/03/22 10:20
S13	1	"20050283837".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S14	1	"20060059238".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S15	1	"20030154399".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S16	4136	IP with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S17	2135	IP adj address$5 with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S18	1427	S17 and (instant adj messag$5 email e?mail e adj mail)	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S19	419	S18 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20

S20	225	S19 not S4	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S21	3994	IP adj address$5 same (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S22	1388	S21 and geographic$5	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S23	377	S22 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S24	213	S23 not S7	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S25	362	S20 S24	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S26	15740	(G06F21/55$ G06F21/56$ H04L29/06551 H04L29/06877-06918 H04L51/12 H04L51/20 H04L63/14-145).cpc.	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S27	6022	S26 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20
S28	356	S27 and IP adj address same match$5	US-PGPUB; USPAT	OR	OFF	2016/03/22 10:20

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S36	177	(match$5 and sender and third adj part$5).clm.	US-PGPUB; USPAT	OR	ON	2016/03/22 10:50
S37	23134	(match$5 and sender and third adj part$5)	US-PGPUB; USPAT	OR	ON	2016/03/22 11:00
S38	5855	S37 and (infect$5 malicious$5 suspicio$7 virus trojan worm)	US-PGPUB; USPAT	OR	ON	2016/03/22 11:00
S39	128	S38 and (rout$5 and consist$5).clm.	US-PGPUB; USPAT	OR	ON	2016/03/22 11:00

3/22/2016 11:05:30 AM
C:\Users\tweidner\Documents\EAST\Workspaces\11237004.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	TIMOTHY J WEIDNER	2476

CPC						
Symbol					**Type**	**Version**
H04L		63	/	1425	F	2013-01-01
H04L		51	/	22	A	2013-01-01
H04L		51	/	20	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/TIMOTHY J WEIDNER/ Primary Examiner.Art Unit 2476	04/08/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	19A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	TIMOTHY J WEIDNER	2476

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
		H	0	4	L	29 / 06 (2006.01.01)						
CROSS REFERENCE(S)		H	0	4	L	12 / 58 (2006.01.01)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/TIMOTHY J WEIDNER/ Primary Examiner.Art Unit 2476	04/08/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	19A

U.S. Patent and Trademark Office

Part of Paper No. 20160322

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	TIMOTHY J WEIDNER	2476

☐ 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		17		33	15	49								
	2		18	2	34		50								
	3		19	3	35		51								
	4		20	4	36	16	52								
	5		21	5	37	17	53								
	6		22	6	38	18	54								
	7		23	7	39										
	8		24	8	40										
	9		25	9	41										
	10		26	10	42										
	11		27		43										
	12		28		44										
	13		29	11	45										
	14		30	12	46										
	15	1	31	13	47										
	16		32	14	48										

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 18	
/TIMOTHY J WEIDNER/ Primary Examiner.Art Unit 2476 (Primary Examiner)	04/08/2016 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 19A

U.S. Patent and Trademark Office Part of Paper No. 20160322

Office of Petitions: Routing Sheet



Application No. 11/237,004

This application is being forwarded to your office for further processing. A decision has been rendered on a petition filed in this application, as indicated below. For details of this decision, please see the document PET.OP.DEC filed on the same date as this document.

[X] **GRANTED**

[ ] **DISMISSED**

[ ] **DENIED**

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 04/05/2016

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER
WEIDNER, TIMOTHY J

ART UNIT	PAPER NUMBER
2476	

MAIL DATE	DELIVERY MODE
04/05/2016	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.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Application of	:	
Roskind et al.	:	
Application No. 11/237,004	:	DECISION ON PETITION
Filed: September 27, 2005	:	PURSUANT TO
Attorney Docket No. PB-036	:	37 C.F.R. § 1.181(a)
Title: DETECTING AND PROCESSING	:	
SUSPICIOUS NETWORK	:	
COMMUNICATIONS	:	

This is a decision on the petition pursuant to 37 C.F.R. § 1.181(a) to withdraw the holding of abandonment, filed on March 3, 2016.

The above-identified application became abandoned for failure to reply in a timely manner to the non-final Office action, mailed June 23, 2015, which set a shortened statutory period for reply of three months. No response was received, and no extensions of time under the provisions of 37 C.F.R. § 1.136(a) were requested. Accordingly, the above-identified application became abandoned on September 24, 2015. A notice of abandonment was mailed on January 19, 2016.

With this petition, Petitioner has alleged that a response was filed on December 23, 2015 along with a three-month extension of time so as to make timely the response.

The electronic file has been reviewed and a response (an amendment to the claims and remarks), a petition for a three-month extension of time so as to make timely the response and the associated $700 fee have each been located in the same. Each of these items was received on December 28, 2015, however it is noted the first page of the amendment contains a certificate of mailing dated December 23, 2015.

Considering the facts and circumstances of the delay at issue, as set forth on petition, it is concluded that Petitioner has met his burden of establishing that a response was timely submitted.

Accordingly, the petition pursuant to 37 C.F.R. § 1.181(a) is **GRANTED**. The holding of abandonment is **WITHDRAWN**.

The Technology Center will be notified of this decision, and jurisdiction over this application is transferred to the Technology Center, so that the application may receive further processing. The Technology Center's support staff will notify the Examiner of this decision, so that the amendments to the claims and remarks (each received on December 28, 2015) can be processed in due course.

Telephone inquiries regarding this decision should be directed to the undersigned at (571) 272-3225.[1] All other inquiries concerning examination procedures or status of the application should be directed to the Technology Center.

/Paul Shanoski/
Paul Shanoski
Attorney Advisor
Office of Petitions

1 Petitioner will note that all practice before the Office should be in writing, and the action of the Office will be based exclusively on the written record in the Office. *See* 37 C.F.R. § 1.2. As such, Petitioner is reminded that no telephone discussion may be controlling or considered authority for any of Petitioner's further action(s).

Office of Petitions: Decision Count Sheet

Mailing Month

Application No. 11237004

11237004

For US serial numbers: enter number only, no slashes or commas. Ex: 10123456
For PCT: enter "51+single digit of year of filing+last 5 numbers", Ex. for PCT/US05/12345, enter 51512345

Deciding Official: Paul Shanoski

Count (1) - Palm Credit 11/237,004

Decision: GRANT

FINANCE WORK NEEDED
☐ Select Check Box for YES

GRANT

Decision Type: 525 - 37 CFR 1.181 for W/D HOLDING OF ABANDONMEN

525

Notes:

Count (2)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Count (3)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Initials of Approving Official (if required)

If more than 3 decisions, attach 2nd count sheet & mark this box

Printed on: *4/1/2016*

Office of Petitions Internal Document - Ver. 5.0

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: March 22, 2016.

/Aaron T. Emigh/
Aaron Emigh

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on March 22, 2016 between the Examiner and the undersigned Applicant.

The Notice of Abandonment dated 1/19/2016 and the Amendment filed December 23, 2015 were discussed.

Applicant inquired as to the status of the application in light of the erroneous Notice of Abandonment that had been discussed in the previous interview. The Examiner confirmed that the application would be revived when he filed a response to the Amendment.

Applicant discussed his belief, as outlined in the Amendment, that the claim amendments in the Amendment overcame the prior art. The Examiner agreed and indicated that the next office action would be a Notice of Allowance.

Applicant wishes to thank the Examiner for his time and attention in this matter.

Electronic Acknowledgement Receipt

EFS ID:	25271493
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	22-MAR-2016
Filing Date:	27-SEP-2005
Time Stamp:	15:55:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant summary of interview with examiner	PB-036-interview-summary-2.pdf	65311 d5056ad2246c9dbbfb6a4ddf72339257829f2a35	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	65311

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 03/14/2016

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	

ART UNIT	PAPER NUMBER
2476	

MAIL DATE	DELIVERY MODE
03/14/2016	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.

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2476	

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

(1) *Timothy J. Weidner*. (3)_____.

(2) *Aaron Emigh (Applicant)*. (4)_____.

Date of Interview: *02 March 2016*.

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: *N/A*.

Identification of prior art discussed: *N/A*.

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...)

Applicant indicated the notice of abandonment on 19 January 2016 to be erroneous based upon the prior response having a receipt date on 28 December 2015 and a certificate of mailing date on 23 December 2015. Agreement was reached on the above matters. The prior response is considered timely based on the certificate of mailing date, as such the previous holding of abandonment is withdrawn.

Applicant recordation instructions: 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

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

/Timothy J Weidner/ Primary Examiner, Art Unit 2476	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Interview record OK /TW/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: March 3, 2016.

/Aaron T. Emigh/
Aaron Emigh

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on March 1, 2016 and continued on March 2, 2016 between the Examiner and the undersigned Applicant.

The Notice of Abandonment dated 1/19/2016 was discussed.

Applicant pointed out that while the Notice of Abandonment states that the Application has been abandoned because no reply to the Office Action sent on June 23, 2015 (the "Office Action") was received, this was in error, because Amendment F was timely filed.

Applicant pointed out that Amendment F is fully responsive to the Office Action and that it was in Private PAIR including a signed Certificate of Mailing certifying that it was mailed on December 23, 2015, and is stamped by the USPTO as having been received on December 28, 2015, consistent with the December 23 mailing date.

The Examiner reviewed the record and stated that he agreed that Amendment F was responsive and had been timely filed, but that it had not been entered into the Examiner's electronic files prior to the issuance of the Notice of Abandonment, and that therefore the Notice of Abandonment was due to a clerical error.

The Examiner stated that he would respond to Amendment F with another Office Action and that the instant application would therefore not be abandoned. Applicant inquired as to

whether he should place something in the file withdrawing the Notice of Abandonment. The Examiner said he would place an interview summary in the file to place the intention to withdraw on the record. Applicant told the Examiner that he may file a Petition to Withdraw the Notice of Abandonment out of an abundance of caution (as he is indeed doing), in order to ensure that no rights are waived in the unlikely event another error was made, with the understanding from the Examiner that such a Petition would likely be mooted by its being reviewed after prosecution had already been reopened, in which event there will be no outstanding Notice of Abandonment to withdraw.

Applicant wishes to thank the Examiner for his time and attention in this matter.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: March 3, 2016.

/Aaron T. Emigh/
Aaron Emigh

RESPONSE TO NOTICE OF ABANDONMENT AND PETITION TO THE DIRECTOR UNDER 37 C.F.R. §1.181 AND MPEP § 711.03(C),I,B.

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

Dear Sir:

This is in response to the Notice of Abandonment mailed January 19, 2016 in the above-identified application.

Applicant respectfully petitions the Director under 37 C.F.R. §1.181 to withdraw the holding of abandonment, which was issued in error. The Notice of Abandonment states that the Application has been abandoned because no reply to the Office Action sent on June 23, 2015 (the "Office Action") was received.

Respectfully, this is in error, as is evident from a review of the file history in Private PAIR. Amendment F, a copy of which is attached hereto, begins "This is in response to the Office Action mailed June 23, 2015" and contains amendments and comments that are fully responsive to all issues raised in the Office Action. Amendment F is in the USPTO's file history

accessible via Private PAIR, contains a signed Certificate of Mailing on page 1 certifying that it was mailed on December 23, 2015, and is stamped by the USPTO as having been received on December 28, 2015, consistent with the December 23 mailing date. Furthermore, Amendment F included an authorization to pay the appropriate Extension of Time fees, and the USPTO accordingly deducted the $700 extension of time fees from Applicant's deposit account no. 504831 on January 8, 2016, further proving that Amendment F was received and processed. A copy of the fee history for the instant application, obtained from Private PAIR, is attached that shows this deduction. Finally, Applicant obtained a Certificate of Mailing from the US Postal Service at the time of mailing, showing that it was indeed mailed from Redwood City, CA on December 23, 2015. A copy is attached hereto. (As an aside, this was filed by Postal Service mail due to the massive site outage experienced by the USPTO on December 22-24, 2015, which rendered EFS inoperable.)

Therefore, it is abundantly clear that Amendment F, a reply to the Office Action, was timely filed and received at the USPTO and was processed accordingly, as demonstrated by the presence of Amendment F in Private PAIR, the Certificate of Mailing signed by Applicant certifying that it was mailed on December 23, 2015, the USPTO date stamp certifying that it was processed on December 28, 2015, the Certificate of Mailing from the US Postal Service proving that it was mailed by the Postal Service on December 23, 2015, and the extension of time fees deducted from Applicant's deposit account in accordance with its filing within the third month.

Accordingly, Applicant respectfully petitions the Director under 37 C.F.R. §1.181 to withdraw the holding of abandonment.

Respectfully submitted,

Dated: March 3, 2016

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

OPAP AKIMA-14
DEC 2 8 2015
PATENT & TRADEMARK OFFICE

IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

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:

December 23, 2015.

Aaron Emigh

AMENDMENT F

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 June 23, 2014. The following amendments and remarks are respectfully submitted.

01/08/2016 APEREZAM 00000004 504831 11237004
01 FC:2253 700.00 DA

IN THE CLAIMS

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

Listing of Claims:

1-30. (canceled)

31. (previously presented) A method, comprising:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if [[when]] it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match.

32. (canceled)

33. (canceled)

34. (previously presented) The method of claim 31, wherein the first routing information includes an IP address.

35. (previously presented) The method of claim 31, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

36. (previously presented) The method of claim 31, wherein the received network communication includes an email message.

37. (previously presented) The method of claim 31, wherein the received network communication includes an instant message.

38. (previously presented) The method of claim 31, wherein the prior network communication includes an email message.

39. (previously presented) The method of claim 31, wherein the network communication is classified as infected because it includes a virus.

40. (previously presented) The method of claim 31, wherein the network communication is classified as infected because it includes a worm.

41. (previously presented) The method of claim 31, wherein the network communication is classified as infected because it includes a Trojan horse.

42. (currently amended) A system, comprising:

a hardware processor configured to:

determine that a received network communication is classified by anti-contagion software as infected;

extract first routing information from the received network communication;

determine whether second routing information from a prior network communication received previously matches the first routing information; and

send a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if [[when]] it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match; and

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

43. (canceled)

44. (canceled)

45. (previously presented) The system of claim 42, wherein the first routing information includes an IP address.

46. (previously presented) The system of claim 42, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

47. (previously presented) The system of claim 42, wherein the received network communication includes an email message.

48. (previously presented) The system of claim 42, wherein the received network communication includes an instant message.

49. (currently amended) A computer program product, embodied in a non-transitory computer readable medium and comprising computer instructions for:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if [[when]] it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match.

50. (canceled)

51. (canceled)

52. (previously presented) The computer program product of claim 49, wherein the first routing information includes an IP address.

53. (previously presented) The computer program product of claim 49, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

54. (previously presented) The computer program product of claim 49, wherein the received network communication includes an email message.

REMARKS

Claims 31, 34-42, 45-49, and 52-54 are pending. Claims 31, 42, and 49 have been amended. Claims 32, 33, 43, 44, 50, and 51 have been canceled. Support for the amendments may be found without limitation at paragraph 57, and Figure 19, of the specification, and in the previously presented claims.

The Examiner has rejected claims 31, 33, 34, 36-39, 42, 44, 45, 47-49, 51, 52, and 54 under 35 USC 102(e) as anticipated by Olivier et al (US 2005/0283837).

Olivier does not teach "sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match," as recited in amended independent claims 31, 42, and 49. Amended independent claims 31, 42, and 49 are therefore believed to be allowable.

Claims 34 and 36-39 depend from claim 31 and are believed to be allowable for the same reasons described above. Claim 33 has been canceled.

Claims 45 and 47-48 depend from claim 42 and are believed to be allowable for the same reasons described above. Claim 44 has been canceled.

Claims 52 and 54 depend from claim 49 and are believed to be allowable for the same reasons described above. Claim 51 has been canceled.

The Examiner has rejected claims 32, 35, 40, 41, 43, 46, 50, and 53 under 35 USC 103(a) as being unpatentable over Olivier in view of of Gleichauf (US 2003/0191966). The Decision on Appeal sustained these rejections. Claims 12, 6, and 12 have been canceled.

Neither Olivier nor Gleichauf, alone or in combination, appear to teach or suggest "sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match," as recited in amended independent claims 31, 42, and 49.

Claims 35, 40, and 41 depend from claim 31 and are therefore believed to be allowable. Claim 32 has been canceled.

Claim 46 depends from claim 42 and is therefore believed to be allowable. Claim 43 has been canceled.

Claim 53 depends from claim 42 and is therefore believed to be allowable. Claim 50 has been canceled.

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: December 23, 2015

Aaron Emigh
Customer #85853

OPAP AKIMA-14
DEC 2 8 2015
PATENT & TRADEMARK OFFICE

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.

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-036).

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/237,004	Filing Date 09/27/2005	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **12/28/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 18	Minus	** 24	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

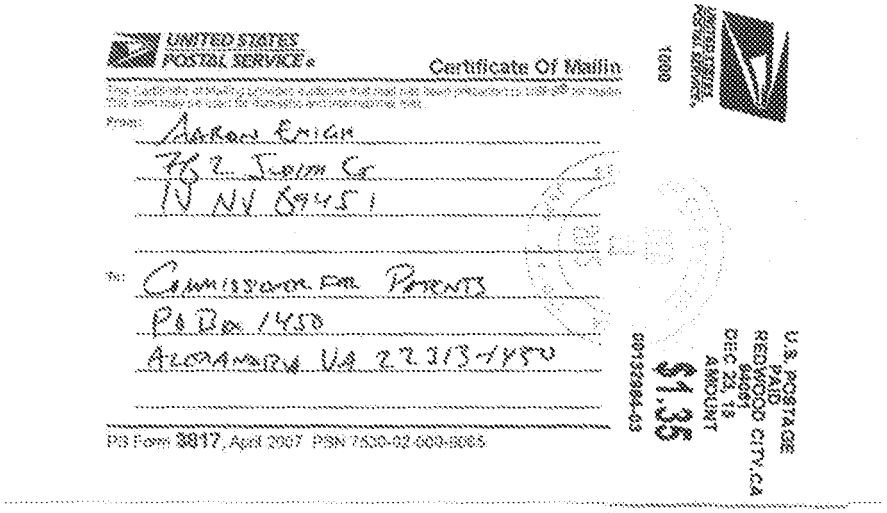
AMENDMENT

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/EVELYN NIMMONS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.


UNITED STATES POSTAL SERVICE
Certificate Of Mailin
From:
Adrian Enlan
76 E. Storm Cr
IV NV 89451
To:
Commissioner for Patents
PO Box 1450
Alexandria VA 22313-1450
PS Form 3817, April 2007 PSN 7530-02-000-9065
U.S. POSTAGE
PAID
REDWOOD CITY, CA
94063
DEC 23, 18
AMOUNT
$1.35

uspto.gov
The United States Patent and Trademark Office
an agency of the Department of Commerce

Patent Application Information Retrieval

Home | Patents | Trademarks | Other | Sign-Off Authenticated Session as Aaron Thompson Emigh

Patent eBusiness

- Electronic Filing
- Patent Application Information (PAIR)
- Patent Ownership
- Fees
- Supplemental Resources & Support

Patent Information

Patent Guidance and General Info
- Codes, Rules & Manuals
- Employee & Office Directories
- Resources & Public Notices

Patent Searches

Patent Official Gazette
- Search Patents & Applications
- Search Biological Sequences
- Copies, Products & Services

Other

Copyrights
Trademarks
Policy & Law
Reports

Secured Patent Application Information Retrieval

Download | Order Certified Application As Filed | Order Certified File Wrapper | View Order List

11/237,004 Detecting and processing suspicious network communications **PB-036**

Select New Case | Application Data | Address & Attorney/Agent | Continuity Data | Fees | Address & Attorney/Agent | Foreign Priority | Transaction History | Image File Wrapper | Continuity Data | Fees | Address & Attorney/Agent | Supplemental Content | Assignments | Display References | Publication Review

Maintenance Fee History

Maintenance Fee data does not exist

Fee Payment History

Accounting Date	Fee Code	Fee Amount	Mailroom Date	Payment Method
01-08-2016	2253	$700.00	12-28-2015	DA 504831
02-05-2015	2202	$40.00	02-02-2015	DA 504831
02-02-2015	2820	$850.00	02-02-2015	DA 504831
02-07-2012	2402	$310.00	02-07-2012	DA 504831
02-07-2012	2254	$990.00	02-07-2012	DA 504831
08-08-2011	2253	$555.00	08-07-2011	DA 504831
08-08-2011	2401	$270.00	08-07-2011	DA 504831
12-06-2010	2202	$78.00	12-03-2010	DA 504831
12-06-2010	2253	$555.00	12-03-2010	DA 504831
01-12-2010	2253	$555.00	01-11-2010	DA 504831
01-12-2010	2801	$405.00	01-11-2010	DA 504831
10-19-2009	8021	$40.00	10-16-2009	DA 504831
10-19-2009	8021	$40.00	10-16-2009	DA 504831
03-09-2009	2252	$245.00	03-09-2009	CK
09-30-2005	2011	$150.00	09-27-2005	CK
09-30-2005	2111	$250.00	09-27-2005	CK
09-30-2005	2311	$100.00	09-27-2005	CK
09-30-2005	2201	$100.00	09-27-2005	CK

If you need help:

- *Contact the Patent Electronic Business Center at (866) 217-9197 (toll free) or e-mail EBC@uspto.gov for specific questions about Patent Application Information Retrieval (PAIR).*
- *If you experience technical difficulties or problems with PAIR outside normal Patent Electronic Business Center hours (M-F, 6AM to 12AM ET), please call 1 800-786-9199.*
- *Send general questions about USPTO programs to the USPTO Contact Center (UCC).*

Accessibility
Privacy Policy
Terms of Use
Security
Emergencies/Security Alerts
Information Quality Guidelines

Federal Activities Inventory Reform (FAIR) Act
Notification and Federal Employee Antidiscrimination and Retaliation (NoFEAR) Act
Budget & Performance
Freedom of Information Act (FOIA)

Department of Commerce NoFEAR Act Report
Regulations.gov
STOPFakes.gov
Department of Commerce
USA.gov
Strategy Targeting Organized Piracy (STOP!)
Careers
Site Index
Contact Us
USPTO Webmaster

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: March 3, 2016.

/Aaron T. Emigh/
Aaron Emigh

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on March 1, 2016 and continued on March 2, 2016 between the Examiner and the undersigned Applicant.

The Notice of Abandonment dated 1/19/2016 was discussed.

Applicant pointed out that while the Notice of Abandonment states that the Application has been abandoned because no reply to the Office Action sent on June 23, 2015 (the "Office Action") was received, this was in error, because Amendment F was timely filed.

Applicant pointed out that Amendment F is fully responsive to the Office Action and that it was in Private PAIR including a signed Certificate of Mailing certifying that it was mailed on December 23, 2015, and is stamped by the USPTO as having been received on December 28, 2015, consistent with the December 23 mailing date.

The Examiner reviewed the record and stated that he agreed that Amendment F was responsive and had been timely filed, but that it had not been entered into the Examiner's electronic files prior to the issuance of the Notice of Abandonment, and that therefore the Notice of Abandonment was due to a clerical error.

The Examiner stated that he would respond to Amendment F with another Office Action and that the instant application would therefore not be abandoned. Applicant inquired as to

whether he should place something in the file withdrawing the Notice of Abandonment. The Examiner said he would place an interview summary in the file to place the intention to withdraw on the record. Applicant told the Examiner that he may file a Petition to Withdraw the Notice of Abandonment out of an abundance of caution (as he is indeed doing), in order to ensure that no rights are waived in the unlikely event another error was made, with the understanding from the Examiner that such a Petition would likely be mooted by its being reviewed after prosecution had already been reopened, in which event there will be no outstanding Notice of Abandonment to withdraw.

Applicant wishes to thank the Examiner for his time and attention in this matter.

Electronic Acknowledgement Receipt

EFS ID:	25085839
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	03-MAR-2016
Filing Date:	27-SEP-2005
Time Stamp:	02:16:37
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	Miscellaneous Incoming Letter	PB-036-abandonment-response-complete.pdf	2250257 25fce034d97511833e16745cbec20d628f2e1f93	no	14

Warnings:	
Information:	

2	Applicant summary of interview with examiner	PB-036-interview-summary.pdf	69984 6bd0f42f7155bd6b5ee472de0d21f7b847a7ed7b	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	2320241	

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 01/19/2016

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER
WEIDNER, TIMOTHY J

ART UNIT	PAPER NUMBER
2476	

MAIL DATE	DELIVERY MODE
01/19/2016	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.

Notice of Abandonment	Application No.	Applicant(s)
	11/237,004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J. Weidner	2476

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

This application is abandoned in view of:

1. ☒ Applicant's failure to timely file a proper reply to the Office letter mailed on *23 June 2015*.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
   (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 to the final rejection.
   (A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) if this is utility or plant application, a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. Note that RCEs are not permitted in design applications.)
   (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
   (d) ☒ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $_____ is insufficient. A balance of $_____ is due.
   The issue fee required by 37 CFR 1.18 is $_____. The publication fee, if required by 37 CFR 1.18(d), is $_____.
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record or other party authorized under 37 CFR 1.33(b). See 37 CFR 1.138(b).

5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34) upon the filing of a continuing application.

6. ☐ The decision by the Board of Patent Appeals and Interference rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☐ The reason(s) below:

/Timothy J Weidner/ Primary Examiner, Art Unit 2476	

Petitions to revive under 37 CFR 1.137, or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

OPAP AKIMA-14
DEC 2 8 2015
PATENT & TRADEMARK OFFICE

IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

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:

December 23, 2015.

Aaron Emigh

AMENDMENT F

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 June 23, 2014. The following amendments and remarks are respectfully submitted.

01/08/2016 APEREZAM 00000004 504831 11237004
01 FC:2253 700.00 DA

IN THE CLAIMS

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

Listing of Claims:

1-30. (canceled)

31. (previously presented) A method, comprising:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if [[when]] it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match.

32. (canceled)

33. (canceled)

34. (previously presented) The method of claim 31, wherein the first routing information includes an IP address.

35. (previously presented) The method of claim 31, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

36. (previously presented) The method of claim 31, wherein the received network communication includes an email message.

37. (previously presented) The method of claim 31, wherein the received network communication includes an instant message.

38. (previously presented) The method of claim 31, wherein the prior network communication includes an email message.

39. (previously presented) The method of claim 31, wherein the network communication is classified as infected because it includes a virus.

40. (previously presented) The method of claim 31, wherein the network communication is classified as infected because it includes a worm.

41. (previously presented) The method of claim 31, wherein the network communication is classified as infected because it includes a Trojan horse.

42. (currently amended) A system, comprising:

a hardware processor configured to:

determine that a received network communication is classified by anti-contagion software as infected;

extract first routing information from the received network communication;

determine whether second routing information from a prior network communication received previously matches the first routing information; and

send a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if [[when]] it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match; and

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

43. (canceled)

44. (canceled)

45. (previously presented) The system of claim 42, wherein the first routing information includes an IP address.

46. (previously presented) The system of claim 42, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

47. (previously presented) The system of claim 42, wherein the received network communication includes an email message.

48. (previously presented) The system of claim 42, wherein the received network communication includes an instant message.

49. (currently amended) A computer program product, embodied in a non-transitory computer readable medium and comprising computer instructions for:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if [[when]] it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match.

50. (canceled)

51. (canceled)

52. (previously presented) The computer program product of claim 49, wherein the first routing information includes an IP address.

53. (previously presented) The computer program product of claim 49, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

54. (previously presented) The computer program product of claim 49, wherein the received network communication includes an email message.

REMARKS

Claims 31, 34-42, 45-49, and 52-54 are pending. Claims 31, 42, and 49 have been amended. Claims 32, 33, 43, 44, 50, and 51 have been canceled. Support for the amendments may be found without limitation at paragraph 57, and Figure 19, of the specification, and in the previously presented claims.

The Examiner has rejected claims 31, 33, 34, 36-39, 42, 44, 45, 47-49, 51, 52, and 54 under 35 USC 102(e) as anticipated by Olivier et al (US 2005/0283837).

Olivier does not teach "sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match," as recited in amended independent claims 31, 42, and 49. Amended independent claims 31, 42, and 49 are therefore believed to be allowable.

Claims 34 and 36-39 depend from claim 31 and are believed to be allowable for the same reasons described above. Claim 33 has been canceled.

Claims 45 and 47-48 depend from claim 42 and are believed to be allowable for the same reasons described above. Claim 44 has been canceled.

Claims 52 and 54 depend from claim 49 and are believed to be allowable for the same reasons described above. Claim 51 has been canceled.

The Examiner has rejected claims 32, 35, 40, 41, 43, 46, 50, and 53 under 35 USC 103(a) as being unpatentable over Olivier in view of of Gleichauf (US 2003/0191966). The Decision on Appeal sustained these rejections. Claims 12, 6, and 12 have been canceled.

Neither Olivier nor Gleichauf, alone or in combination, appear to teach or suggest "sending a notification that the received network communication was classified as infected, wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, wherein the recipient is selected as the sender associated with the prior network communication if it is determined that the first routing information and the second routing information match, and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match," as recited in amended independent claims 31, 42, and 49.

Claims 35, 40, and 41 depend from claim 31 and are therefore believed to be allowable. Claim 32 has been canceled.

Claim 46 depends from claim 42 and is therefore believed to be allowable. Claim 43 has been canceled.

Claim 53 depends from claim 42 and is therefore believed to be allowable. Claim 50 has been canceled.

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: December 23, 2015



Aaron Emigh
Customer #85853

OPAP AKIMA-14
DEC 2 8 2015
PATENT & TRADEMARK OFFICE

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.

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-036).

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/237,004	Filing Date 09/27/2005	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT	12/28/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 24	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

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

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

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

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

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

LIE
/EVELYN NIMMONS/

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/237,004	Filing Date 09/27/2005	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **12/28/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 18	Minus	** 24	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

SLIE
/DIANIECE JACOBS/

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 06/23/2015

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER
WEIDNER, TIMOTHY J

ART UNIT	PAPER NUMBER
2476	

MAIL DATE	DELIVERY MODE
06/23/2015	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. 11/237,004	Applicant(s) ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2476	AIA (First Inventor to File) Status No

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

Period for Reply

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

- Extensions of time may be available under the provisions of 37 CFR 1.136(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 *02/02/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

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

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

Disposition of Claims*

5)☒ Claim(s) *31-54* 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) *31-54* is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

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)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Patent Trial and Appeal Board, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 02/02/2015 has been entered.

Response to Amendment and Remarks

In response to the amendment on 02/02/2015, the status of the claims is as follows. Claims 1-20 are cancelled. Claims 31-54 are new and pending.

In response to the remarks on 02/02/2015, the arguments have been considered but they are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

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

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

Claims 31, 33, 34, 36-39, 42, 44, 45, 47-49, 51, 52 and 54 are rejected under pre-AIA 35 U.S.C. 102(e) as being anticipated by Olivier et al. (US 2005/0283837).

31. (new) A method, comprising:

(*Olivier*, paragraph [0056], "FIG. 2 is a flow diagram of a process of generating a count of suspicious messages, according to an embodiment. In one implementation, the steps of FIG. 2 may be performed by a virus information source, such as virus information source 104 in FIG. 1.")

determining that a received network communication is classified by anti-contagion software as infected;

(*Olivier*, paragraph [0059], "The determination that a message is suspicious also may be made by extracting a source network address from the message, such as a source IP value, and issuing a query to the SenderBase service to determine whether the source is known to be associated with spam or viruses.")

extracting first routing information from the received network communication;

(*Olivier*, paragraph [0059], "The determination that a message is suspicious also may be made by extracting a source network address from the message, such as a source IP value, and issuing a query to the SenderBase service to determine whether the source is known to be associated with spam or viruses.")

determining whether second routing information from a prior network communication received previously matches the first routing information; and

(*Olivier*, paragraph [0059], "The determination that a message is suspicious also may be made by extracting a source network address from the message, such as a

source IP value, and issuing a query to the SenderBase service to determine whether the source is known to be associated with spam or viruses.")

sending a notification that the received network communication was classified as infected, when it is determined that the first routing information and the second routing information match.

(*Olivier*, paragraph [0059], "The determination that a message is suspicious also may be made by extracting a source network address from the message, such as a source IP value, and issuing a query to the SenderBase service to determine whether the source is known to be associated with spam or viruses." paragraph [0062], "In step 208, the count of suspicious messages is reported. For example, step 208 may involve sending a report message to the virus information processor 108.")

33. (new) The method of claim 31, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication.

(*Olivier*, paragraph [0063], "In an embodiment, virus information processor 108 receives numerous reports such as the report of step 208, continuously in real time. As reports are received, virus information processor 108 updates database 112 with report data, and determines and stores virus outbreak information. In one embodiment, the virus outbreak information includes a virus score value that is determined according to a sub-process that is described further with reference to FIG. 4 below.")

34. (new) The method of claim 31, wherein the first routing information includes an IP address.

(*Olivier*, paragraph [0059], "The determination that a message is suspicious also may be made by extracting a source network address from the message, such as a source IP value, and issuing a query to the SenderBase service to determine whether the source is known to be associated with spam or viruses.")

36. (new) The method of claim 31, wherein the received network communication includes an email message.

(*Olivier*, paragraph [0034], "FIG. 1 is a block diagram of a system for managing computer virus outbreaks, according to an embodiment. A virus sender 100, whose identity and location are typically unknown, sends a message infected with a virus, typically in an electronic message, or email, with a virus-bearing executable file attachment, to public network 102, such as the Internet. The message is either addressed to, or propagates by action of the virus to, a plurality of destinations such as virus information source 104 and spamtrap 106. A spamtrap is an email address or an email mailbox used to collect information about unsolicited email messages. The operation and implementation of virus information source 104 and spamtrap 106 is discussed in further detail below. For purposes of illustrating a simple example, FIG. 1 shows only two destinations in the form of virus information source 104 and spamtrap 106, but in a practical embodiment there may be any number of such sources of virus information.")

37. (new) The method of claim 31, wherein the received network communication includes an instant message.

(*Olivier*, paragraph [0034], "FIG. 1 is a block diagram of a system for managing computer virus outbreaks, according to an embodiment. A virus sender 100, whose identity and location are typically unknown, sends a message infected with a virus, typically in an electronic message, or email, with a virus-bearing executable file attachment, to public network 102, such as the Internet. The message is either addressed to, or propagates by action of the virus to, a plurality of destinations such as virus information source 104 and spamtrap 106. A spamtrap is an email address or an email mailbox used to collect information about unsolicited email messages. The operation and implementation of virus information source 104 and spamtrap 106 is discussed in further detail below. For purposes of illustrating a simple example, FIG. 1 shows only two destinations in the form of virus information source 104 and spamtrap 106, but in a practical embodiment there may be any number of such sources of virus information.")

38. (new) The method of claim 31, wherein the prior network communication includes an email message.

(*Olivier*, paragraph [0034], "FIG. 1 is a block diagram of a system for managing computer virus outbreaks, according to an embodiment. A virus sender 100, whose identity and location are typically unknown, sends a message infected with a virus, typically in an electronic message, or email, with a virus-bearing executable file attachment, to public network 102, such as the Internet. The message is either

addressed to, or propagates by action of the virus to, a plurality of destinations such as virus information source 104 and spamtrap 106. A spamtrap is an email address or an email mailbox used to collect information about unsolicited email messages. The operation and implementation of virus information source 104 and spamtrap 106 is discussed in further detail below. For purposes of illustrating a simple example, FIG. 1 shows only two destinations in the form of virus information source 104 and spamtrap 106, but in a practical embodiment there may be any number of such sources of virus information.")

39. (new) The method of claim 31, wherein the network communication is classified as infected because it includes a virus.

(*Olivier*, paragraph [0059], "The determination that a message is suspicious also may be made by extracting a source network address from the message, such as a source IP value, and issuing a query to the SenderBase service to determine whether the source is known to be associated with spam or viruses. For example, a reputation score value provided by the SenderBase service may be taken into account in determining whether a message is suspicious. A message may also be determined to be suspicious if it was sent from an IP address associated with a host known to be compromised, that has a history of sending viruses, or has only recently started sending email to the Internet. The determination also may be based upon one or more of the following factors: (a) the type or extension of a file attachment that is directly attached to the message, (b) the type or extension of a file that is contained within a compressed

file, an archive, a .zip file, or another file that is directly attached to the message, and (c) a data fingerprint obtained from an attachment.")

42. (new) A system (cf. claim 31), comprising:

a hardware processor configured to:

determine that a received network communication is classified by anti- contagion software as infected;

extract first routing information from the received network communication;

determine whether second routing information from a prior network communication received previously matches the first routing information; and

send a notification that the received network communication was classified as infected, when it is determined that the first routing information and the second routing information match; and

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

44. (new) The system of claim 42, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication (cf. claim 33).

45. (new) The system of claim 42, wherein the first routing information includes an IP address (cf. claim 34).

47. (new) The system of claim 42, wherein the received network communication includes an email message (cf. claim 36).

48. (new) The system of claim 42, wherein the received network communication includes an instant message (cf. claim 37).

49. (new) A computer program product, embodied in a non-transitory computer readable medium and comprising computer instructions (cf. claim 31) for:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, when it is determined that the first routing information and the second routing information match.

51. (new) The computer program product of claim 49, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication (cf. claim 33).

52. (new) The computer program product of claim 49, wherein the first routing information includes an IP address (cf. claim 34).

54. (new) The computer program product of claim 49, wherein the received network communication includes an email message (cf. claim 36).

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 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.

Claims 32, 35, 40, 41, 43, 46, 50 and 53 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Olivier et al. (US 2005/0283837) as applied to claims 31, 42 and 49 above, and further in view of Gleichauf (US 2003/0191966).

32. (new) The method of claim 31, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

(*Gleichauf*, paragraph [0045], "In operation, once a damaging element is detected, communication protocol shim 42 may send a signal directly to infected computer 18 that signifies that infective element 12 is within its internal structure. Infected computer 18 may then respond to the signal by communicating with remediator website 30, or alternatively by performing some cleaning or security check for its corresponding internal structure.")

35. (new) The method of claim 31, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

(*Gleichauf*, paragraph [0048], "As described above, communication protocol shim 42 may generate a signal that includes numerous pieces of information that relate to the presence of infective element 12. For example, the signal may include the location of infective element 12 as given by a corresponding address (possibly an IP address) of where infective element 12 resides. In addition, the signal generated and communicated by communication protocol shim 42 may include information relating to the type of damaging element that has entered the system. Also, the signal may include information for remedial measures for coping with or for combating the damaging element. For example, certain damaging elements may be eliminated from the system by a simple deletion instruction, whereas others may need more complex instructions for how to combat their presence. Alternatively, the signal generated by communication protocol shim 42 may include any other suitable information that offers some guidance in handling the presence or harmful affects of infective element 12.")

40. (new) The method of claim 31, wherein the network communication is classified as infected because it includes a worm.

(*Gleichauf*, paragraph [0042], "Virus detection element 40 is an element or an object capable of detecting a damaging element after it has entered communication system 10. Virus detection element 40 may be a collection of routines or programs that execute pattern matching, looking for specific or systematic traffic behavior. Data packet patterns may provide a medium for which damaging elements within a system's architecture may be identified. Virus detection element 40 may include any hardware, software, or elements operable to detect a damaging element, such as infective element

12, present in communication system 10. Virus detection element 40 may also be a desktop firewall product, such as those produced by Symantec Inc., Network Associates, or Computer Associates that perform some (potentially routine) security screening in insuring that a corresponding element is clean of potential harmful elements. Virus detection element 40 may also be capable of identifying a particular type of damaging element, such as a Trojan, a worm, or a virus, for example. Virus detection element 40 may communicate information associated with the type of damaging element introduced into communication system 10 to communication protocol shim 42, to network management controller 14, or to any other suitable location. Each of computers 16a-16c may also include any suitable element operable to facilitate, or otherwise execute the disabling of a communications capability of infected computer 18.")

41. (new) The method of claim 31, wherein the network communication is classified as infected because it includes a Trojan horse.

(*Gleichauf*, paragraph [0042], "Virus detection element 40 is an element or an object capable of detecting a damaging element after it has entered communication system 10. Virus detection element 40 may be a collection of routines or programs that execute pattern matching, looking for specific or systematic traffic behavior. Data packet patterns may provide a medium for which damaging elements within a system's architecture may be identified. Virus detection element 40 may include any hardware, software, or elements operable to detect a damaging element, such as infective element 12, present in communication system 10. Virus detection element 40 may also be a

desktop firewall product, such as those produced by Symantec Inc., Network Associates, or Computer Associates that perform some (potentially routine) security screening in insuring that a corresponding element is clean of potential harmful elements. Virus detection element 40 may also be capable of identifying a particular type of damaging element, such as a Trojan, a worm, or a virus, for example. Virus detection element 40 may communicate information associated with the type of damaging element introduced into communication system 10 to communication protocol shim 42, to network management controller 14, or to any other suitable location. Each of computers 16a-16c may also include any suitable element operable to facilitate, or otherwise execute the disabling of a communications capability of infected computer 18.")

43. (new) The system of claim 42, wherein sending the notification includes sending the notification to a sender associated with the prior network communication (cf. claim 32).

46. (new) The system of claim 42, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region (cf. claim 35).

50. (new) The computer program product of claim 49, wherein sending the notification includes sending the notification to a sender associated with the prior network communication (cf. claim 32).

53. (new) The computer program product of claim 49, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region (cf. claim 35).

The teachings, suggestions, and motivations of *Olivier* and *Gleichauf* are self-evident from the citations relied upon herein. Their objectives are summarized as prior art techniques for improved network security and data protection. As such, it would have been obvious to a person having a level of ordinary skill in the pertinent art, at the time the disclosed invention was made, to combine the teachings of *Olivier* and *Gleichauf* and to arrive at the subject matter of claims 32, 35, 40, 41, 43, 46, 50 and 53, in order to improve network security and data protection.

Conclusion

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Timothy J. Weidner whose telephone number is (571)270-1825. The examiner can normally be reached on Monday - Friday, 8:00 AM - 5:00 PM, Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Timothy J Weidner/
Primary Examiner
Art Unit 2476

Notice of References Cited	Application/Control No. 11/237,004	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2476	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0154399 A1	08-2003	Zuk et al.	713/201
*	B	US-2003/0191966 A1	10-2003	Gleichauf, Robert E.	713/201
*	C	US-2005/0169274 A1	08-2005	Shuster, Gary Stephen	370/392
*	D	US-2005/0283837 A1	12-2005	Olivier et al.	726/024
*	E	US-2006/0031483 A1	02-2006	Lund et al.	709/224
*	F	US-2006/0059238 A1	03-2006	Slater et al.	709/206
*	G	US-2006/0288076 A1	12-2006	Cowings et al.	709/206
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1415	IP with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	USPAT	OR	OFF	2015/06/18 15:06
S2	735	IP adj address$5 with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	USPAT	OR	OFF	2015/06/18 15:06
S3	481	S2 and (instant adj messag$5 email e?mail e adj mail)	USPAT	OR	OFF	2015/06/18 15:06
S4	188	S3 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	USPAT	OR	OFF	2015/06/18 15:06
S5	1399	IP adj address$5 same (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	USPAT	OR	OFF	2015/06/18 15:06
S6	438	S5 and geographic$5	USPAT	OR	OFF	2015/06/18 15:06
S7	157	S6 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	USPAT	OR	OFF	2015/06/18 15:06
S8	5725	(G06F21/55$ G06F21/56$ H04L29/06551 H04L29/06877-06918 H04L51/12 H04L51/20 H04L63/14-145).cpc.	USPAT	OR	OFF	2015/06/18 15:06
S9	2816	S8 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	USPAT	OR	OFF	2015/06/18 15:06
S10	798	S9 and IP adj address	USPAT	OR	OFF	2015/06/18 15:06
S11	546	S10 and match$5	USPAT	OR	OFF	2015/06/18 15:06
S12	160	S11 and IP adj address same match$5	USPAT	OR	OFF	2015/06/18 15:06
S13	1	"20050283837".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:06
S14	1	"20060059238".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:06
S15	1	"20030154399".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:06
S16	3645	IP with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:09
S17	1797	IP adj address$5 with (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:09
S18	1188	S17 and (instant adj messag$5 email e?mail e adj mail)	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:10
S19	408	S18 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:11

S20	220	S19 not S4	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:16
S21	3440	IP adj address$5 same (infect$5 malicious$5 suspicio$7 virus trojan worm) and match$5	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:16
S22	1160	S21 and geographic$5	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:17
S23	363	S22 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:17
S24	206	S23 not S7	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:17
S25	352	S20 S24	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:18
S26	13465	(G06F21/55$ G06F21/56$ H04L29/06551 H04L29/06877-06918 H04L51/12 H04L51/20 H04L63/14-145).cpc.	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:19
S27	5817	S26 and (@ad<"20050927" @prad<"20050927" @rlad<"20050927")	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:19
S28	349	S27 and IP adj address same match$5	US-PGPUB; USPAT	OR	OFF	2015/06/18 15:20

EAST Search History (Interference)

< This search history is empty>

6/ 18/ 2015 4:02:46 PM
C:\ Users\ tweidner\ Documents\ EAST\ Workspaces\ 11237004.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J Weidner	2476

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
eDAN inventorship search	9/25/2008	TJW
EAST search class/sub 370/252,389,401 713/153,154 726/22,26,27 using keywords	9/29/2008	TJW
eDAN and EAST searches above updated	7/7/2009	TJW
EAST keyword search	7/7/2009	TJW
eDAN and EAST searches above updated	5/28/2010	TJW
EAST keyword search	5/28/2010	TJW
eDAN and EAST searches above updated	2/15/2011	TJW
EAST keyword search	2/15/2011	TJW
USPAT and US-PGPUB search using limited classification	6/18/2015	TJW

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: February 2, 2015.

/Aaron T. Emigh/
Aaron Emigh

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL FILED WITH AMENDMENT E

This is a Request for Continued Examination (RCE) under 37 CFR §1.114 of the above-identified application.

1. Submission required under 37 CFR §1.114

a. ☒ Enclosed:

- ☒ Amendment/Reply
- ☐ Affidavit(s)/Declaration(s)
- ☐ Information Disclosure Statement (IDS)
- ☐ Other

Respectfully submitted,

Dated: February 2, 2015

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2nd and Subsequent Request	2820	1	850	850
		Total in USD ($)		**850**

Electronic Acknowledgement Receipt

EFS ID:	21367120
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	02-FEB-2015
Filing Date:	27-SEP-2005
Time Stamp:	06:10:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$850
RAM confirmation Number	8984
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-036-amendment-e-rce.pdf	106864 3cf1ae27f8eb0dee9018cb80e0c9b66ac116395b	yes	7

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Argument after Patent Board Decision	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	6
Request for Continued Examination (RCE)	7	7

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30303 d8327982650a6439fbef116da2864a429883e33e	no	2

Warnings:

Information:

Total Files Size (in bytes):	137167

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:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: February 2, 2015.

/Aaron T. Emigh/
Aaron Emigh

AMENDMENT E

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

Dear Sir:

This is in response to the Decision on Appeal mailed December 3, 2014. 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:

1-30. (canceled)

31. (new) A method, comprising:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, when it is determined that the first routing information and the second routing information match.

32. (new) The method of claim 31, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

33. (new) The method of claim 31, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication.

34. (new) The method of claim 31, wherein the first routing information includes an IP address.

35. (new) The method of claim 31, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

36. (new) The method of claim 31, wherein the received network communication includes an email message.

37. (new) The method of claim 31, wherein the received network communication includes an instant message.

38. (new) The method of claim 31, wherein the prior network communication includes an email message.

39. (new) The method of claim 31, wherein the network communication is classified as infected because it includes a virus.

40. (new) The method of claim 31, wherein the network communication is classified as infected because it includes a worm.

41. (new) The method of claim 31, wherein the network communication is classified as infected because it includes a Trojan horse.

42. (new) A system, comprising:

a hardware processor configured to:

determine that a received network communication is classified by anti-contagion software as infected;

extract first routing information from the received network communication;

determine whether second routing information from a prior network communication received previously matches the first routing information; and

send a notification that the received network communication was classified as infected, when it is determined that the first routing information and the second routing information match; and

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

43. (new) The system of claim 42, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

44. (new) The system of claim 42, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication.

45. (new) The system of claim 42, wherein the first routing information includes an IP address.

46. (new) The system of claim 42, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

47. (new) The system of claim 42, wherein the received network communication includes an email message.

48. (new) The system of claim 42, wherein the received network communication includes an instant message.

49. (new) A computer program product, embodied in a non-transitory computer readable medium and comprising computer instructions for:

determining that a received network communication is classified by anti-contagion software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information; and

sending a notification that the received network communication was classified as infected, when it is determined that the first routing information and the second routing information match.

50. (new) The computer program product of claim 49, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

51. (new) The computer program product of claim 49, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication.

52. (new) The computer program product of claim 49, wherein the first routing information includes an IP address.

53. (new) The computer program product of claim 49, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

54. (new) The computer program product of claim 49, wherein the received network communication includes an email message.

REMARKS

Claims 31-54 are pending. Claims 1-30 have been canceled. New claims 31-54 have been added. Support for the new claims can be found without limitation at paragraph 57, and Figure 19A, of the specification.

The Examiner has rejected claims 1, 3, 6, 8, 11, 13, and 25-27 under 35 USC 103(a) as being unpatentable over Bandini et al (US 2002/0199095) in view of of Sobel et al (US 7,366,919). The Decision on Appeal sustained these rejections. Claims 1, 3, 6, 8, 11, 13, and 25-27 have been canceled. Neither Bandini nor Sobel, alone or in combination, appear to teach or suggest the claimed limitations of new claims 31-54. New claims 31-54 are therefore believed to be allowable.

The Examiner has rejected claims 2, 7, and 12 under 35 USC 103(a) as being unpatentable over Bandini in view of of Sobel , further in view of Kirsch (US 2005/0198159). The Decision on Appeal sustained these rejections. Claims 12, 6, and 12 have been canceled. Neither Bandini, Sobel, nor Kirsch, alone or in combination, appear to teach or suggest the claimed limitations of new claims 31-54. New claims 31-54 are therefore believed to be allowable.

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: February 2, 2015

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/237,004	Filing Date 09/27/2005	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **02/02/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 24	Minus	** 23	= 1	X $40 =	40
Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	40

AMENDMENT

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

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

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

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

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

LIE
/VIKKI GRAY/

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

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

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 02/05/2015

YSHORT SALE #00000006 Mailroom Dt: 02/02/2015 504831 11237004
01 FC : 2202 40.00 DA

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 12/03/2014

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	

ART UNIT	PAPER NUMBER
2476	

MAIL DATE	DELIVERY MODE
12/03/2014	PAPER

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

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JAMES A. ROSKIND and AARON T. EMIGH

Appeal 2012-008660
Application 11/237,004
Technology Center 2400

Before LEE E. BARRETT, STANLEY M. WEINBERG, and DANIEL J. GALLIGAN, *Administrative Patent Judges*.

GALLIGAN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants[1] seek our review under 35 U.S.C. § 134(a) of the Examiner's rejection of claims 1–3, 6–8, 11–13, and 25–27. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.[2]

---

[1] The Appeal Brief identifies Radix Holdings, LLC as the real party in interest. App. Br. 2.

[2] Our Decision refers to Appellants' Appeal Brief filed on February 7, 2012 ("App. Br."); Appellants' Reply Brief filed May 9, 2012; Examiner's Answer mailed March 16, 2012 ("Ans."); and original Specification filed September 27, 2005 ("Spec.").

STATEMENT OF THE CASE

Claims on Appeal

Claims 1, 6, and 11 are independent claims. Claim 1 is reproduced below:

> 1. A method for identifying a message as suspicious, comprising:
>
> extracting from a received email message a sender of the received message, wherein the sender is an email address;
>
> determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;
>
> retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;
>
> determining whether the first source IP address and the second source IP address are associated with the same geographical region; and
>
> identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

Examiner's Rejections[3]

Claims 1, 3, 6, 8, 11, 13, and 25–27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bandini[4] and Sobel.[5] Ans. 4–12.

---

[3] Although Appellants identify the rejection of claims 11–13 under 35 U.S.C. § 101 as a ground to be reviewed (App. Br. 4–5), the Examiner stated that this rejection was withdrawn by the Advisory Action dated August 25, 2011 (Ans. 12–13). As such, we do not address this rejection.
[4] Bandini et al., U.S. Patent App. Publication 2001/0199195 A1, published Dec. 26, 2002 (hereinafter "Bandini").
[5] Sobel et al., U.S. Patent 7,366,919 B1, issued Aug. 29, 2008 (hereinafter "Sobel").

Claims 2, 7, and 12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bandini, Sobel, and Kirsch.[6] Ans. 12.

ANALYSIS

Appellants contend the combination of Bandini and Sobel does not teach or suggest the limitation of independent claims 1, 6, and 11 reciting "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox." App. Br. 6–8.

The Examiner found the "SPAM database" of Bandini teaches a "spam inbox." Ans. 5 (citing Bandini ¶ 22). Appellants argue that Bandini's "SPAM database" does not teach "an inbox," as recited in the claims. App. Br. 6–7. Appellants cite various pieces of extrinsic evidence and argue: "An inbox, as is known to one skilled in the art, is a term specifically referring to the main repository for incoming emails that are intended for a user to read." App. Br. 7. Appellants further argue that "'spam inbox' is an oxymoron" because a spam filter diverts email from an inbox. App. Br. 7. In reply, Appellants still further argue various characteristics of an inbox in an attempt to distinguish Bandini's "SPAM database" from the claimed "an inbox." Reply Br. 15–16.

We are not persuaded by Appellants' arguments. First, as the Examiner pointed out, Appellants' Specification and one of the pending claims use the term "spam inbox." Ans. 13–14 (citing claim 25 and Spec. ¶ 56). Appellants' Specification states: "Another example of restricting impact or further scrutiny of a message may include placing a message in a

[6] U.S. Patent App. Publication 2005/0198159 A1, published Sept. 8, 2005.

spam inbox." Spec. ¶ 56. Furthermore, Appellants rely on limitations of "an inbox" that are not recited in the claims. The claims in a patent provide the metes and bounds of the exclusive rights the patent confers on the patentee. *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257 (Fed. Cir. 1989). Arguments for patentability not based on the limitations actually recited in the claims are not persuasive. *In re Self*, 671 F.2d 1344, 1348 (CCPA 1982). In addition, Appellants do not direct us to persuasive evidence, such as a specific definition in the Specification, that the term should be interpreted as restrictively as Appellants contend. We note that Appellants' Specification uses the term "inbox" only a few times, once as part of the term "spam inbox." *See* Spec. ¶¶ 56, 57. As such, we are not persuaded that the Examiner erred in finding that the "SPAM database" of Bandini teaches "an inbox."

Appellants also argue that Bandini teaches away from the invention because the "SPAM database" is in an email relay, which cannot have an inbox. App. Br. 8; Reply Br. 17–18. We are not persuaded because the claims do not recite that the "inbox" must be located in any particular location or computer system.

Based on the foregoing, we sustain the rejection of independent claims 1, 6, and 11. Appellants do not advance additional persuasive arguments for patentability of dependent claims 2, 3, 7, 8, 12, 13, and 25–27. App. Br. 8–10. Therefore, for the reasons above, we sustain the rejection of dependent claims 3, 8, 13, and 25–27 under 35 U.S.C. § 103(a) over Bandini and Sobel, and we sustain the rejection of dependent claims 2, 7, and 12 under 35 U.S.C. § 103(a) over Bandini, Sobel, and Kirsch.

DECISION

We affirm the Examiner's rejection of claims 1–3, 6–8, 11–13, and 25–27.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

rwk

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 05/24/2012

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	
ART UNIT	PAPER NUMBER
2476	
MAIL DATE	DELIVERY MODE
05/24/2012	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.

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

AARON EMIGH

762 JUDITH COURT

INCLINE VILLAGE, NV 89451

Appeal No: 2012-008660
Application: 11/237,004
Appellant: James A. Roskind et al.

Board of Patent Appeals and Interferences
Docketing Notice

Application 11/237,004 was received from the Technology Center at the Board on May 21, 2012 and has been assigned Appeal No: 2012-008660.

In all future communications regarding this appeal, please include both the application number and the appeal number.

The mailing address for the Board is:

BOARD OF PATENT APPEALS AND INTERFERENCES
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VIRGINIA 22313-1450

The facsimile number of the Board is 571-273-0052. Because of the heightened security in the Washington D.C. area, facsimile communications are recommended. Telephone inquiries can be made by calling 571-272-9797 and referencing the appeal number listed above.

By order of the Board of Patent Appeals and Interferences.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: May 9, 2012.

/Aaron T. Emigh/
Aaron Emigh

APPELLANT'S REPLY BRIEF PURSUANT TO 37 C.F.R. §41.41

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, replies to the Examiner's Answer mailed on March 16, 2012.

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 1-3, 6-8, 11-13, and 25-27 are currently pending in the application, and are attached hereto as an appendix. 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 D, filed on August 7, 2011, are believed to have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Since the application is being prosecuted *pro se*, **the summary of claimed subject matter is not required according to 37 CFR 41.37(c)(1).** Accordingly, this summary section provides not an authoritative summary but rather guidance to aid in understanding embodiments of the claimed subject matter.

In general, the independent claims are directed toward processing a received email message by determining routing data associated with that message, including an IP address, and comparing the geographic region of the IP address with the geographic region of a second IP address which is part of routing data associated with a previously received email message from the same sender, which is in an inbox. The received email is then identified as suspicious if the geographic regions do not match.

An effect of this, in essence, is to compare where an email was sent from, or routed through, with previous email from the same sender which is reasonably assumed to be authentic (e.g. not spam), because it was either delivered to the user's inbox instead of being routed elsewhere by a spam filter, or moved to the inbox by the user because it was deemed to be authentic. Spammers do not generally operate mail servers in the same geographic regions as an entity they are spamming, so this can be an effective measure in combating spam. For example, if previous emails from Amazon.com have been delivered and are routed from Seattle, Washington, and a new email comes in which is routed from Moscow, it would be wise to treat this as suspicious.

As can readily be seen, there is a significant benefit to the claimed techniques, which are a novel approach to geographic filtering of email messages in comparison to previously received email messages which are presumed to be authentic by virtue of their presence in an inbox – namely, improved identification of spam.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 11-13 are unpatentable under 35 U.S.C §101 as directed to unpatentable subject matter.

Whether claims 1, 3, 6, 8, 11, 13, and 25-27 are unpatentable under 35 U.S.C §103(a) over Bandini et al (U.S. 2002/0199095), hereinafter referred to as Bandini, in view of Sobel et al (U.S. Patent No. 7,366,919), hereinafter referred to as Sobel.

Whether claims 2, 7, and 12 are unpatentable under 35 U.S.C. §103(a) over Bandini in view of Sobel, further in view of Kirsch (U.S. 2005/0198159).

VII. ARGUMENT

WHETHER CLAIMS 11-13 ARE UNPATENTABLE UNDER 35 U.S.C §101 AS DIRECTED TO UNPATENTABLE SUBJECT MATTER

In the Final Office Action, the Examiner suggested language to overcome his rejection of claims 11-13. Applicant incorporated the Examiner's suggestion into Amendment D, which was entered by the Examiner. Therefore, Applicant believes that this controversy has been resolved and respectfully requests the Examiner to withdraw his rejection under 35 U.S.C. §101.

WHETHER CLAIMS 1, 3, 6, 8, 11, 13, AND 25-27 ARE UNPATENTABLE UNDER 35 U.S.C §103(A) OVER BANDINI IN VIEW OF SOBEL

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 Claims 1, 3, 6, 8, 11, 13, and 25-27. The MPEP, section 2141, states that:

> *An invention that would have been obvious to a person of ordinary skill at the time of the invention is not patentable. See 35 U.S.C. 103(a). As reiterated by the Supreme Court in KSR, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries. The factual inquiries enunciated by the Court are as follows:*
>
> *(A) Determining the scope and content of the prior art;*
>
> *(B) Ascertaining the differences between the claimed invention and the prior art; and*
>
> *(C) Resolving the level of ordinary skill in the pertinent art.*

The Examiner has erred in two of the three factual inquiries of the process outlined above. He has (A) mischaracterized the scope and content of the prior art, in that he has mischaracterized a prior art reference as teaching material it does not; and has (B) failed to ascertain the differences between the claimed invention and the prior art, as a consequence of that mischaracterization.

Claims 1, 6, and 11

The Examiner erred in rejecting claims 1, 6, and 11 because the combination of Bandini and Sobel do not render "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox" obvious because the Examiner has misconstrued an "inbox."

The Examiner has relied upon Bandini, paragraph 32 as teaching "wherein the prior email message is in an inbox," within the above-mentioned limitation. In the instant application, this is used, for example, to compare routing data for an incoming message with one reasonably believed to be authentic, because it is in an email inbox. Bandini not only does not teach this, but in fact teaches away from it, because Bandini's teachings are specific to a prior email address being used being in a SPAM database in an email relay, which cannot be an inbox. The Examiner has cited Bandini, paragraph 32, quoting "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message." This explicitly teaches that an incoming message is compared with a known spam message, not with a message in an inbox. Acknowledging this, the Examiner states that "SPAM database treated as spam inbox."

Respectfully, "spam inbox" is an oxymoron. An inbox, as is known to one skilled in the art, is a term specifically referring to the main repository for incoming emails that are intended for a user to read. If spam filtering has been applied, then it diverts emails *away from* the inbox, either to a junk mail folder, a spam database, or by simple deletion. For example, the definition of "inbox" on the Tech Terms Computer Dictionary states that "An inbox is the main folder that your incoming mail gets stored in… it is common to create other folders to store your messages…" (Retrieved on February 6, 2012 from http://www.techterms.com/definition/inbox.) Here, there is a distinct division between an inbox (the *main folder* that your incoming mail gets stored in) and other folders, such as a spam folder. This distinction is perfectly clear, for example, in the documentation provided by Microsoft for Outlook, the most popular email client: "Microsoft Office Outlook 2007 contains a Junk E-mail Filter designed to ***reduce the unwanted e-mail presented in your inbox***. The junk e-mail, also known as spam, is ***routed by the filter instead to a Junk E-mail folder***, where it can be more effectively managed." (Microsoft Corporation, "Overview of the Junk E-mail Filter," retrieved on February 6, 2012 from http://office.microsoft.com/en-us/outlook-help/overview-of-the-junk-e-mail-filter-HP001230028.aspx; emphasis added.) Here as elsewhere, Microsoft uses the term "inbox" in the sense that one skilled in the art necessarily would, as the main repository of (hopefully non-spam) email for a user to review; and specifically distinguishes this from the "junk email folder" into which spam is filtered. Therefore, the Examiner's construal of a "spam database" as an "inbox" is unreasonable.

Therefore, the Examiner erred in rejecting claims 1, 6, and 11 under 35 U.S.C. §103(a) as unpatentable over Bandini in view of Sobel.

The Examiner erred in rejecting claims 1, 6, and 11 because the combination of Bandini and Sobel do not render "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox" obvious because Bandini teaches that a "SPAM database" exists not on an email server but on an email relay, which cannot have an inbox

The Examiner's construal of a "SPAM database" as an "inbox" is not only oxymoronic, but also is taught away from by Bandini, because Bandini architecturally places the "SPAM database" where no inbox could exist. Specifically, in Bandini, the described filtering takes place on an "email relay" that is not on a mail server, and which therefore is incapable of hosting an inbox. See, for example, Bandini, paragraph 11: "The e-mail relay 46 advantageously takes a form as described in further detail herein to filter e-mail messages received from outside the protected enterprise." Figure 1 of Bandini clearly shows e-mail relay 46 as a distinct component between public network 44 and email server 40, which would normally hold an inbox. Paragraph 13 continues: "The ***e-mail relay 46 has available a SPAM database 37*** and a message store 38, which is typically used to store e-mail messages ***while in transit***." So in addition to the fact that a "SPAM database" cannot logically be construed as an "inbox," according to Bandini, the "SPAM database" is kept on e-mail relay 46, which is (per Bandini, Figure 1) an architecturally separate component from the email server used to filter email *while in transit*, and cannot possible store an inbox (which would, in Bandini, be stored on Mail Server 40, which is accessed by User Stations 34, 36 to obtain email).

Therefore, the Examiner erred in rejecting claims 1, 6, and 11 under 35 U.S.C. §103(a) as unpatentable over Bandini in view of Sobel.

Claims 3 and 25-27

Claims 3 and 25-27 depend from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejections of claims 3 and 25-27. Therefore, those rejections are also erroneous.

Claim 8

Claim 8 depends from claim 6. As discussed above, the Examiner's rejection of claim 6 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 8. Therefore, this rejection is also erroneous.

Claim 13

Claim 13 depends from claim 11. As discussed above, the Examiner's rejection of claim 11 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 13. Therefore, this rejection is also erroneous.

WHETHER CLAIMS 2, 7, AND 12 ARE UNPATENTABLE UNDER 35 U.S.C. §103(A) OVER BANDINI IN VIEW OF SOBEL, FURTHER IN VIEW OF KIRSCH

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 Claims 2, 7, and 12.

Claim 2

Claim 2 depends from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 2. Therefore, this rejection is also erroneous.

Claim 7

Claim 7 depends from claim 6. As discussed above, the Examiner's rejection of claim 6 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 7. Therefore, this rejection is also erroneous.

Claim 12

Claim 12 depends from claim 11. As discussed above, the Examiner's rejection of claim 11 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 12. Therefore, this rejection is also erroneous.

VIII. CLAIMS APPENDIX

1. A method for identifying a message as suspicious, comprising:

extracting from a received email message a sender of the received message, wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

2. A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

6. A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received email message a sender of the received message, wherein the sender is an email address;

determine a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determine whether the first source IP address and the second source IP address are associated with the same geographical region; and

identify the received message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region; and

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

7. A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

11. A computer program product for identifying a message as suspicious, the computer program product being embodied in a non-transitory computer readable storage medium and comprising computer instructions for:

extracting from a received email message a sender of the received message, wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

12. A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

25. The method of claim 1, further comprising placing the received email message in a spam inbox, when the received email message is identified as suspicious.

26. The method of claim 1, further comprising preventing execution of content contained in the received email message, when the received email message is identified as suspicious.

27. The method of claim 1, further comprising presenting a warning that describes a circumstance associated with the identification of the received email message as suspicious.

IX. EVIDENCE APPENDIX

Not Applicable.

X. RELATED PROCEEDINGS APPENDIX

Not Applicable.

XI. RESPONSE TO ARGUMENTS

Whether Bandini teaches away from processing an email message in an inbox

The Examiner argues that Bandini does not "teach away" from processing a prior email message in an inbox, although it teaches such processing being done on an email relay server which architecturally cannot host an inbox, because Bandini does not "discredit, criticize, or otherwise discourage the solution claimed." Appellant respectfully notes that Bandini's performance of email processing on an email relay server dramatically "discourages" the solution claimed, in that it renders it impossible.

Whether a "spam database" discloses an inbox

The Examiner argues that a "spam database," as taught by Bandini, discloses an "inbox." Respectfully, this construction, which is at the heart of the rejection of the independent claims, is improper, for multiple reasons which are individually set forth below.

First reason why a "SPAM database" does not disclose an "inbox": A "database" is a much more general term, while an "inbox" has a more specific meaning, which is not disclosed by Bandini, and for which which Bandini's implementation is inappropriate

A database is a general term for any organized collection of data. An inbox, on the other hand, is a more specific term used by those skilled in the art (as well as in general usage) to refer to a folder used to store incoming electronic messages for a single user, who can then review the messages in the inbox, respond to them, etc. Respectfully, there is no teaching in Bandini that a "SPAM database" would be an inbox. For example, Bandini's "SPAM database" does not afford any opportunity for users to review emails in it; it is simply used for comparison of attributes. (See, for example, Bandini, paragraphs 20 and 23, and Figure 2, reference numeral 54, and Figure 3, reference numeral 66.) Indeed, there is no indication in Bandini that any inbox-specific functionality would be provided by the "SPAM database," nor any other indication that the "SPAM database" could be an inbox.

Indeed, the only implementation of the "SPAM database" taught in Bandini (paragraph 24) is "a relational database such as an Oracle or SQL server… The message body is preferably

stored as a Character Large Object or as a Binary Large Object in the message record, as in known in the art. In another embodiment, the message body is stored in one or more other records, which are associated with the master message data record, such as by employing a master-detail pattern relationship. The message recipient identifiers for each message are preferably stored in a different table, where records are associated with corresponding master message data records, as is known in the art." Clearly, this is a description of an implementation of a database that is purpose-built for searching based on particular attributes rather than for user review, and again there is no indication that the "SPAM database" of Bandini would, or could, be an inbox.

Second reason why a "SPAM database" does not disclose an "inbox": Bandini teaches storing data in the "SPAM database" that is incompatible with an inbox

In Bandini, the "SPAM database" is not storing incoming email for a single user, as an inbox does, but rather email that has been sent to *multiple* users, which has been reviewed (i.e. is no longer incoming) and found to be SPAM. It is therefore neither used to store *incoming* email, nor email for a *single* user. (See for example Bandini, paragraphs 30 and 34-38, and Figure 4.)

Furthermore, the data stored in the "SPAM database" of Bandini includes data that would not reasonably be included in an inbox. For example, as taught in Bandini, paragraph 25, "Information that is derived by processing of the known SPAM messages is also stored in the database 37. In one embodiment, a hash computation result based on the message body, or portions of the message body, is stored in the database 37... This hash value is used by the e-mail relay 46 to quickly determine a match likelihood between a received message body text and a known SPAM message body text. Other data derived from the SPAM messages include URLs found in the message body. These URLs can be stored in a URL table, where records are associated with corresponding SPAM message records by a master-detail pattern relationship." This type of data would not be included in the implementation of an inbox, as it serves no purpose for user retrieval and review of email, and hence the "spam database" described in Bandini is not in fact an inbox, as construed by the Examiner.

Third reason why a "SPAM database" does not disclose an "inbox": Bandini teaches that the "SPAM database" is on a relay server, which architecturally cannot host an inbox

Bandini architecturally places the "SPAM database" where no inbox could exist. Specifically, in Bandini, the described filtering using the "SPAM database" takes place on an "email relay" that is not on a mail server or email client machine, and which therefore is incapable of hosting an inbox – yet it either contains the "SPAM database" or is the only component connected to it. See, for example, Bandini, paragraph 11: "The e-mail relay 46 advantageously takes a form as described in further detail herein to filter e-mail messages received from outside the protected enterprise." Figure 1 of Bandini clearly shows E-mail Relay 46 as a distinct component between Public Network 44 and Email Server 40. Email Server 40, which would normally hold an inbox, is *not* connected to SPAM Database 37, and nor are User Stations 24, 36. Paragraph 13 continues: "The ***e-mail relay 46 has available a SPAM database 37*** and a message store 38, which is typically used to store e-mail messages ***while in transit***." So Bandini's "SPAM database" is either kept on the e-mail relay itself, or coupled only to the email relay and *not* to either the email server or email clients (the "User Stations"). This email relay is an architecturally separate component from the email server, that is used to filter email *while in transit*, and cannot possibly store or provide user access to an inbox (which would, again, be stored on Bandini's Mail Server 40, which is accessed by User Stations 34, 36 to obtain email – neither of which is connected to SPAM Database 37 in Bandini, Figure 1).

The Examiner argues in his Answer that Bandini discloses an email relay server hosting an inbox because (emphasis added) "Appellant's own application provides the claim can be performed for and on intermediate nodes, including mail transfer agents (e.g. specification [0056], 'routing information for an email message may be deduced by examining header information ***relating to*** mail transfer agents…***similarity in IP addresses*** for mail transfer agents may be interpreted as implying similar routing…In some embodiments, the process of Figure 18 is implemented on a mail, messaging, or other server associated with the sender and/or sender's ISP…the recipient and/or the recipient's ISP; and/or one or more intermediate nodes.'" Respectfully, this argument does not hold water for at least three reasons. First, in the emphasized terms, the header information and IP address information merely *relates to* mail transfer agents, and is not necessarily stored there. Second, nowhere in the specification is

performing the process on an *email relay server* as in Bandini disclosed. Third and fundamentally, the fact that the *process* shown in Figure 18 and described in the specification may be performed in a variety of places has no bearing on where the inbox itself is stored, which cannot, for example, be in (or exclusively coupled with) an email relay server as Bandini teaches for its "SPAM database." Rather, in a hypothetical implementation of the claimed invention in which the *processing* was performed on some "intermediate node," the inbox would be remotely accessed from where it was stored (e.g. on an email server), whereas in Bandini, as shown in his Figure 1, the "SPAM database" must be stored on or immediately coupled to a relay server, and inaccessible to an email server or client. Therefore, the Examiner's argument is fatally flawed.

A note on the (ir)relevance of whether a "spam inbox" is a meaningful term

Appellant notes that while he opined that the term "spam inbox," introduced by the Examiner in the Final Office Action, was a malapropism, the Examiner is correct that the term does occur once in the specification. While Appellant believes this term would more aptly be expressed as a spam *folder*, its appearance in the specification does not detract from the arguments above, as the term "spam inbox" does not occur in Bandini, but rather was simply used by the Examiner in the Final Office Action. The legitimacy or illegitimacy of the term "spam inbox" does not bear in any way on the question of whether a "SPAM database" (which is the exclusive term used in Bandini) discloses an inbox, as argued by the Examiner. As explained above in detail, it does not.

Whether Kirsch can be used to overcome the failure of the combination of Bandini and Sobel to render the claimed invention obvious

The Examiner argues that even if the preponderance of the evidence does in fact weigh in Appellant's favor, Kirsch teaches certain (other) processing of emails in inboxes, and therefore, in combination with Bandini and Sobel, could potentially render claims 1, 6, and 11 obvious.

However, the Examiner did not cite Kirsch in his rejection of the instant application. 37 C.F.R. §1.104(c)(2) states that "In rejecting claims for want of novelty or for obviousness, ***the examiner must cite the best references at his or her command***." (Emphasis added.) If the Examiner believes that Kirsch is among the best references at his command to render the claimed

invention obvious, then he was required to cite Kirsch, which he did not, and therefore the rejection is erroneous.

In principle, the Examiner could have cited a combination including Kirsch as a new ground for rejection for claims 1, 6, and 11 in his Answer. However, he did not do so. 37 C.F.R. §41.39(b) refers to "a rejection ***designated as a new ground of rejection***." (Emphasis added.) The MPEP, §1207.03, states that "Any new ground of rejection made by an examiner in an answer must be: (A) approved by a Technology Center (TC) Director or designee; and (B) prominently identified in the 'Grounds of Rejection to be Reviewed on Appeal' section and the 'Grounds of Rejection' section of the answer." The Examiner did not so identify Kirsch as a new ground for rejection for claims 1, 6, and 11 in either section of the Answer, nor was any approval by a Technology Center Director or designee provided. Therefore, since a combination including Kirsch was not designated as a new ground of rejection, it should not be so considered. (As an aside, Appellant further notes that such a hypothetical adding of Kirsch as a new grounds of rejection – which the Examiner did not do – would actually be improper because Kirsch was already known to the Examiner prior to the Final Office Action, and if Kirsch was required for the rejection, then the Examiner failed to cite the best references at his command in the Final Office Action as required under 37 C.F.R. §1.104(c)(2) – which would mean that the rejection was erroneous in the first place.)

In short, there is no scenario in which a combination including Kirsch should be considered for claims 1, 6, and 11, because Kirsch has not been designated as a ground for rejection of those claims, and such a designation, even if it was made (which it was not), would be improper.

For the above reasons, it is believed that the rejection should be reversed.

Respectfully submitted,

Dated: May 9, 2012

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Acknowledgement Receipt

EFS ID:	12744072
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	09-MAY-2012
Filing Date:	27-SEP-2005
Time Stamp:	23:03:16
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	Reply Brief Filed	PB-036-appeal-reply-brief.pdf	202790 ee6b1748a9da1d930f2e4fec2f2de6ccaa82f 113	no	19

Warnings:	
Information:	

Total Files Size (in bytes):	202790

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 03/16/2012

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	
ART UNIT	PAPER NUMBER
2476	
MAIL DATE	DELIVERY MODE
03/16/2012	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.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 11/237,004
Filing Date: September 27, 2005
Appellant(s): ROSKIND ET AL.

Aaron Emigh
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 7, 2012 appealing from the Office action mailed February 18, 2011 as modified by the Advisory Action mailed August 25, 2011.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-3, 6-8, 11-13, and 25-27.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

US 2002/0199095 A1	Bandini et al.	12-2002
US 7,366,919 B1	Sobel et al.	4-2008
US 2005/0198159 A1	Kirsch	9-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3, 6, 8, 11, 13, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bandini et al. (US 2002/0199095 A1) in view of Sobel et al. (US 7366919 B1).

Regarding claim 1, Bandini teaches a method for identifying a message as suspicious (limitations in the preamble are not given patentable weight unless referred to in the body of the claim and addressed below, see MPEP 2111.02), comprising:

extracting from a received email message a sender of the received message, wherein the sender is an email address (paragraph 27, "the sender address of the incoming e-mail message is compared to …");

determining current routing data associated with the received email address, wherein the current routing data includes a first source IP address (paragraph 32, "the

Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of incoming message is treated as first source IP address);

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of SPAM is treated as second source IP address; paragraph 22, SPAM database treated as spam inbox);

determining whether the first source IP address and the second source IP address match (paragraph 32, "a match of the IP address or internet domain would enhance a finding of likely SPAM");

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address match (paragraph 32, "a match of the IP address or internet domain would enhance a finding of likely SPAM").

Bandini may not explicitly teach, but Sobel, which is in the same field of endeavor, teaches:

determining whether the first source IP address and the second source IP address are associated with the same geographical region (column 5, line 59 - column 6, line 1, "address 22 is resolved into a location … If the actual geo-location obtained in step 12 matches one of these resolved locations ..." where a match is treated as

association with the same geographical region; column 5, lines 15-20, where the addresses are source IP addresses); and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If, on the other hand, the actual geo-location obtained from step 12 does not match one of these resolved locations, a declaration is made at step 16 that e-mail 24 contains suspected spam” where not matching is treated as not associated with the same geographical region).

The purpose of Sobel is to reduce the amount of spam to which a computer is subjected (column 1, lines 6-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Bandini, e.g. have “determining … and identifying …” as claimed, to reduce the amount of spam to which a computer is subjected.

Regarding claim 3, Bandini teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 24, “fields of the record preferably correspond to the message header fields").

Regarding claim 6, Bandini teaches a system for identifying a message as suspicious (limitations in the preamble are not given patentable weight unless referred to in the body of the claim and addressed below, see MPEP 2111.02), comprising:

a processor (paragraph 11) configured to:

extract from a received email message a sender of the received message, wherein the sender is an email address (paragraph 27, "the sender address of the incoming e-mail message is compared to …");

determine current routing data associated with the received email address, wherein the current routing data includes a first source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of incoming message is treated as first source IP address);

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of SPAM is treated as second source IP address; paragraph 22, SPAM database treated as spam inbox);

determine whether the first source IP address and the second source IP address match (paragraph 32, "a match of the IP address or internet domain would enhance a finding of likely SPAM");

identify the received email message as suspicious if it is determined that the first source IP address and the second source IP address match (paragraph 32, "a match of the IP address or internet domain would enhance a finding of likely SPAM").

Bandini may not explicitly teach, but Sobel, which is in the same field of endeavor, teaches:

determine whether the first source IP address and the second source IP address are associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If the actual geo-location obtained in step 12 matches one of these resolved locations ..." where a match is treated as association with the same geographical region; column 5, lines 15-20, where the addresses are source IP addresses); and

identify the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If, on the other hand, the actual geo-location obtained from step 12 does not match one of these resolved locations, a declaration is made at step 16 that e-mail 24 contains suspected spam” where not matching is treated as not associated with the same geographical region).

The purpose of Sobel is to reduce the amount of spam to which a computer is subjected (column 1, lines 6-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Bandini, e.g. have “determine … and identify …” as claimed, to reduce the amount of spam to which a computer is subjected.

Regarding claim 8, Bandini teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 24, “fields of the record preferably correspond to the message header fields").

Regarding claim 11, Bandini teaches a computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable storage medium and comprising computer instructions (paragraph 11) (limitations in the preamble are not given patentable weight unless referred to in the body of the claim and addressed below, see MPEP 2111.02) for:

extracting from a received email message a sender of the received message, wherein the sender is an email address (paragraph 27, “the sender address of the incoming e-mail message is compared to …”);

determining current routing data associated with the received email address, wherein the current routing data includes a first source IP address (paragraph 32, “the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message” where IP address of incoming message is treated as first source IP address);

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address (paragraph 32, “the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message” where IP

address of SPAM is treated as second source IP address; paragraph 22, SPAM database treated as spam inbox);

determining whether the first source IP address and the second source IP address match (paragraph 32, “a match of the IP address or internet domain would enhance a finding of likely SPAM”);

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address match (paragraph 32, “a match of the IP address or internet domain would enhance a finding of likely SPAM”).

Bandini may not explicitly teach, but Sobel, which is in the same field of endeavor, teaches:

determining whether the first source IP address and the second source IP address are associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If the actual geo-location obtained in step 12 matches one of these resolved locations ..." where a match is treated as association with the same geographical region; column 5, lines 15-20, where the addresses are source IP addresses); and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If, on the other hand, the actual geo-location obtained from step 12 does not match one of these resolved locations, a declaration is made at step 16 that e-

mail 24 contains suspected spam" where not matching is treated as not associated with the same geographical region).

The purpose of Sobel is to reduce the amount of spam to which a computer is subjected (column 1, lines 6-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Bandini, e.g. have "determining … and identifying …" as claimed, to reduce the amount of spam to which a computer is subjected.

Regarding claim 13, Bandini teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 24, "fields of the record preferably correspond to the message header fields").

Regarding claim 25, Bandini teaches placing the received email message in a spam inbox, when the received email message is identified as suspicious (paragraph 19, "quarantine the e-mail in the local message store database" where database is treated as spam inbox).

Regarding claim 26, Bandini teaches preventing execution of content contained in the received email message, when the received email message is identified as suspicious (paragraph 19, "quarantine the e-mail in the local message store database" where quarantine is treated as preventing execution of content; paragraph 31, where quarantined message including URL is treated as content not executed).

Regarding claim 27, Bandini teaches presenting a warning that describes a circumstance associated with the identification of the received email message as

suspicious (paragraph 19, "generate a special message to the intended recipient indicating that the e-mail message has been diverted").

Claims 2, 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bandini et al. (US 2002/0199095 A1) in view of Sobel et al. (US 7366919 B1), as applied to claims 1, 6, and 11 respectively above, and further in view of Kirsch (US 2005/0198159 A1).

Regarding claims 2, 7, and 12, Bandini may not explicitly teach, but Kirsch, which is in the same field of endeavor, teaches processing the received message normally if it is determined that no prior routing data associated with the sender is available (figure 2, steps 102, 106, 114, 104 in sequence and associated text, where determining sender is not on whitelist or blacklist is treated as determining no prior routing data associated with the sender is available, and sending the email to the recipient is treated as processing the message normally). The purpose of Kirsch is to more effectively filter unwanted e-mails (paragraph 9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kirsch with Bandini and Sobel, e.g. have "processing the received message normally if it is determined that no prior routing data associated with the sender is available" as claimed, to more effectively filter unwanted e-mails.

(10) Response to Argument

Argument, page 5, regarding claims previously rejected under 35 USC 101, have been considered, but they are moot in view of the Advisory Action dated August 25,

2011, which entered the amendment filed August 7, 2011 indicating the rejections under 35 USC 101 had been withdrawn.

Argument, pages 6-10, regarding rejections under 35 USC 103, have been considered, but they are not persuasive for the reasons given below.

A) Argument, pages 6-7, states “Examiner has misconstrued ‘inbox’ … Bandini not only does not teach this, but in fact teaches away from it, because Bandini's teachings are specific to a prior email address being used being in a SPAM database in an email relay, which cannot be an inbox. The Examiner has cited Bandini, paragraph 32 …” Examiner respectfully disagrees. Bandini’s teaching does not “teach away” because Bandini does not "discredit, criticize, or otherwise discourage the solution claimed". *In re Fulton*, 391 F.3d 1195, 1201,73 USPQ2d 1141, 1146 (Fed. Cir. 2004). Therefore, the argument is not persuasive.

B) Argument, page 7, states “Examiner states that ‘SPAM database [is] treated as spam inbox.’ Respectfully, ‘spam inbox’ is an oxymoron. An inbox, as is known to one skilled in the art, is a term specifically referring to the main repository for incoming emails that are intended for a user to read. If spam filtering has been applied, then it diverts emails away from the inbox, either to a junk email folder, a spam database, or by simple deletion." Examiner respectfully disagrees. The limitation "inbox” is given a broadest reasonable interpretation (MPEP 2111). The teaching of a "spam inbox" is within the scope of "inbox" as claimed, i.e. “spam inbox" is a more specific teaching than “inbox”, as indicated by the appellant’s own application (e.g. claim 25, “placing the received email

message in a spam inbox"; specification [0056], “placing a message in a spam inbox”). Further, the teaching of a spam database is within the scope of "inbox" and "spam inbox” (e.g. arguments, page 7, "If spam filtering has been applied, then it diverts emails away from the inbox, either to a junk email folder, a spam database …"; specification [0056], "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”). Therefore, the argument is not persuasive.

C) Argument, page 7, states "the definition of 'inbox' ..." and cites Tech Terms Computer Dictionary and documentation for Microsoft Outlook 2007. However, such external documentation carries little weight when the appellant’s own application provides "spam inbox" as a more specific type of inbox (e.g. claim 25, “placing the received email message in a spam inbox"; specification [0056], “placing a message in a spam inbox”). Further, the cited documentation appears to have publication dates (around 2007) after the application’s filing date (9/27/05, provisional filing 9/27/04). As such, the cited technical documentation does not sufficiently capture the knowledge of one of ordinary skill in the art at the time the application was filed. Therefore, the argument is not persuasive.

D) Argument, page 8, states “The Examiner’s construal of a ‘SPAM database’ as an ‘inbox’ … is taught away from by Bandini because Bandini architecturally places the ‘SPAM database' where no inbox could exist. Specifically, in Bandini, the described filtering takes place on an 'email relay' ..."

Examiner respectfully disagrees. Bandini's teaching does not "teach away" because Bandini does not "discredit, criticize, or otherwise discourage the solution claimed". *In re Fulton*, 391 F.3d 1195, 1201,73 USPQ2d 1141, 1146 (Fed. Cir. 2004). Further, the appellant's own application provides the claim can be performed for and on intermediate nodes, including mail transfer agents (e.g. specification [0056], "routing information for an email message may be deduced by examining header information related to mail transfer agents … similarity in IP addresses for mail transfer agents may be interpreted as implying similar routing ... In some embodiments, the process of Figure 18 is implemented on a mail, messaging, or other server associated with the sender and/or sender's ISP ... the recipient and/or the recipients ISP; and/or one or more intermediate nodes"). Therefore, the argument is not persuasive.

E) Arguments, pages 8-10, repeat the rationales addressed in A)-D) above. Therefore, rationales provided by A)-D) are equally applicable here.

F) Further, even if assuming arguendo that the preponderance of evidence with respect to the appealed grounds of rejection (Bandini in view of Sobel) weighed in the appellant's favor, then consider the third cited reference (Kirsch), applied to claims 2, 7, and 12 (and previously applied to claims 1, 6, and 11 in the office action dated June 3, 2010). Kirsch, teaches the prior email message is in an inbox (paragraph 24, "folders of saved messages may also be checked to construct the whitelist"; paragraph 58, "the whitelist is constructed as above ... messages in the e-mail program's "Inbox" ... are analyzed ... to see if

any are messages from a sender (or site) on the whitelist") for the purpose of more effectively filtering unwanted e-mails based on sender information (paragraph 9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kirsch with Bandini and Sobel, e.g. have the prior email message is in an inbox, to provide a more effective approach to more effectively filter unwanted e-mails based on sender information.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Timothy J Weidner/
Examiner, Art Unit 2476

Conferees:

/PHIRIN SAM/
Primary Examiner, Art Unit 2476

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2476

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: February 7, 2012.

/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 1-3, 6-8, 11-13, and 25-27 set forth in the final Office Action mailed on February 18, 2011.

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 1-3, 6-8, 11-13, and 25-27 are currently pending in the application, and are attached hereto as an appendix. 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 D, filed on August 7, 2011, are believed to have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Since the application is being prosecuted *pro se*, **the summary of claimed subject matter is not required according to 37 CFR 41.37(c)(1).** Accordingly, this summary section provides not an authoritative summary but rather guidance to aid in understanding embodiments of the claimed subject matter.

In general, the independent claims are directed toward processing a received email message by determining routing data associated with that message, including an IP address, and comparing the geographic region of the IP address with the geographic region of a second IP address which is part of routing data associated with a previously received email message from the same sender, which is in an inbox. The received email is then identified as suspicious if the geographic regions do not match.

An effect of this, in essence, is to compare where an email was sent from, or routed through, with previous email from the same sender which is reasonably assumed to be authentic (e.g. not spam), because it was either delivered to the user's inbox instead of being routed elsewhere by a spam filter, or moved to the inbox by the user because it was deemed to be authentic. Spammers do not generally operate mail servers in the same geographic regions as an entity they are spamming, so this can be an effective measure in combating spam. For example, if previous emails from Amazon.com have been delivered and are routed from Seattle, Washington, and a new email comes in which is routed from Moscow, it would be wise to treat this as suspicious.

As can readily be seen, there is a significant benefit to the claimed techniques, which are a novel approach to geographic filtering of email messages in comparison to previously received email messages which are presumed to be authentic by virtue of their presence in an inbox – namely, improved identification of spam.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 11-13 are unpatentable under 35 U.S.C §101 as directed to unpatentable subject matter.

Whether claims 1, 3, 6, 8, 11, 13, and 25-27 are unpatentable under 35 U.S.C §103(a) over Bandini et al (U.S. 2002/0199095), hereinafter referred to as Bandini, in view of Sobel et al (U.S. Patent No. 7,366,919), hereinafter referred to as Sobel.

Whether claims 2, 7, and 12 are unpatentable under 35 U.S.C. §103(a) over Bandini in view of Sobel, further in view of Kirsch (U.S. 2005/0198159).

VII. ARGUMENT

WHETHER CLAIMS 11-13 ARE UNPATENTABLE UNDER 35 U.S.C §101 AS DIRECTED TO UNPATENTABLE SUBJECT MATTER

In the Final Office Action, the Examiner suggested language to overcome his rejection of claims 11-13. Applicant incorporated the Examiner's suggestion into Amendment D, which was entered by the Examiner. Therefore, Applicant believes that this controversy has been resolved and respectfully requests the Examiner to withdraw his rejection under 35 U.S.C. §101.

WHETHER CLAIMS 1, 3, 6, 8, 11, 13, AND 25-27 ARE UNPATENTABLE UNDER 35 U.S.C §103(A) OVER BANDINI IN VIEW OF SOBEL

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 Claims 1, 3, 6, 8, 11, 13, and 25-27. The MPEP, section 2141, states that:

> *An invention that would have been obvious to a person of ordinary skill at the time of the invention is not patentable. See 35 U.S.C. 103(a). As reiterated by the Supreme Court in KSR, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries. The factual inquiries enunciated by the Court are as follows:*
>
> *(A) Determining the scope and content of the prior art;*
>
> *(B) Ascertaining the differences between the claimed invention and the prior art; and*
>
> *(C) Resolving the level of ordinary skill in the pertinent art.*

The Examiner has erred in two of the three factual inquiries of the process outlined above. He has (A) mischaracterized the scope and content of the prior art, in that he has mischaracterized a prior art reference as teaching material it does not; and has (B) failed to ascertain the differences between the claimed invention and the prior art, as a consequence of that mischaracterization.

Claims 1, 6, and 11

The Examiner erred in rejecting claims 1, 6, and 11 because the combination of Bandini and Sobel do not render "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox" obvious because the Examiner has misconstrued an "inbox."

The Examiner has relied upon Bandini, paragraph 32 as teaching "wherein the prior email message is in an inbox," within the above-mentioned limitation. In the instant application, this is used, for example, to compare routing data for an incoming message with one reasonably believed to be authentic, because it is in an email inbox. Bandini not only does not teach this, but in fact teaches away from it, because Bandini's teachings are specific to a prior email address being used being in a SPAM database in an email relay, which cannot be an inbox. The Examiner has cited Bandini, paragraph 32, quoting "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message." This explicitly teaches that an incoming message is compared with a known spam message, not with a message in an inbox. Acknowledging this, the Examiner states that "SPAM database treated as spam inbox."

Respectfully, "spam inbox" is an oxymoron. An inbox, as is known to one skilled in the art, is a term specifically referring to the main repository for incoming emails that are intended for a user to read. If spam filtering has been applied, then it diverts emails *away from* the inbox, either to a junk mail folder, a spam database, or by simple deletion. For example, the definition of "inbox" on the Tech Terms Computer Dictionary states that "An inbox is the main folder that your incoming mail gets stored in… it is common to create other folders to store your messages…" (Retrieved on February 6, 2012 from http://www.techterms.com/definition/inbox.) Here, there is a distinct division between an inbox (the *main folder* that your incoming mail gets stored in) and other folders, such as a spam folder. This distinction is perfectly clear, for example, in the documentation provided by Microsoft for Outlook, the most popular email client: "Microsoft Office Outlook 2007 contains a Junk E-mail Filter designed to ***reduce the unwanted e-mail presented in your inbox***. The junk e-mail, also known as spam, is ***routed by the filter instead to a Junk E-mail folder***, where it can be more effectively managed." (Microsoft Corporation, "Overview of the Junk E-mail Filter," retrieved on February 6, 2012 from http://office.microsoft.com/en-us/outlook-help/overview-of-the-junk-e-mail-filter-HP001230028.aspx; emphasis added.) Here as elsewhere, Microsoft uses the term "inbox" in the sense that one skilled in the art necessarily would, as the main repository of (hopefully non-spam) email for a user to review; and specifically distinguishes this from the "junk email folder" into which spam is filtered. Therefore, the Examiner's construal of a "spam database" as an "inbox" is unreasonable.

Therefore, the Examiner erred in rejecting claims 1, 6, and 11 under 35 U.S.C. §103(a) as unpatentable over Bandini in view of Sobel.

The Examiner erred in rejecting claims 1, 6, and 11 because the combination of Bandini and Sobel do not render "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox" obvious because Bandini teaches that a "SPAM database" exists not on an email server but on an email relay, which cannot have an inbox

The Examiner's construal of a "SPAM database" as an "inbox" is not only oxymoronic, but also is taught away from by Bandini, because Bandini architecturally places the "SPAM database" where no inbox could exist. Specifically, in Bandini, the described filtering takes place on an "email relay" that is not on a mail server, and which therefore is incapable of hosting an inbox. See, for example, Bandini, paragraph 11: "The e-mail relay 46 advantageously takes a form as described in further detail herein to filter e-mail messages received from outside the protected enterprise." Figure 1 of Bandini clearly shows e-mail relay 46 as a distinct component between public network 44 and email server 40, which would normally hold an inbox. Paragraph 13 continues: "The ***e-mail relay 46 has available a SPAM database 37*** and a message store 38, which is typically used to store e-mail messages ***while in transit***." So in addition to the fact that a "SPAM database" cannot logically be construed as an "inbox," according to Bandini, the "SPAM database" is kept on e-mail relay 46, which is (per Bandini, Figure 1) an architecturally separate component from the email server used to filter email *while in transit*, and cannot possible store an inbox (which would, in Bandini, be stored on Mail Server 40, which is accessed by User Stations 34, 36 to obtain email).

Therefore, the Examiner erred in rejecting claims 1, 6, and 11 under 35 U.S.C. §103(a) as unpatentable over Bandini in view of Sobel.

Claims 3 and 25-27

Claims 3 and 25-27 depend from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejections of claims 3 and 25-27. Therefore, those rejections are also erroneous.

Claim 8

Claim 8 depends from claim 6. As discussed above, the Examiner's rejection of claim 6 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 8. Therefore, this rejection is also erroneous.

Claim 13

Claim 13 depends from claim 11. As discussed above, the Examiner's rejection of claim 11 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 13. Therefore, this rejection is also erroneous.

WHETHER CLAIMS 2, 7, AND 12 ARE UNPATENTABLE UNDER 35 U.S.C. §103(A) OVER BANDINI IN VIEW OF SOBEL, FURTHER IN VIEW OF KIRSCH

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 Claims 2, 7, and 12.

Claim 2

Claim 2 depends from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 2. Therefore, this rejection is also erroneous.

Claim 7

Claim 7 depends from claim 6. As discussed above, the Examiner's rejection of claim 6 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 7. Therefore, this rejection is also erroneous.

Claim 12

Claim 12 depends from claim 11. As discussed above, the Examiner's rejection of claim 11 under 35 U.S.C §103(a) was erroneous. The Examiner relied on this erroneous rejection in his rejection of claim 12. Therefore, this rejection is also erroneous.

VIII. CLAIMS APPENDIX

1. A method for identifying a message as suspicious, comprising:

extracting from a received email message a sender of the received message, wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

2. A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

6. A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received email message a sender of the received message, wherein the sender is an email address;

determine a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determine whether the first source IP address and the second source IP address are associated with the same geographical region; and

identify the received message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region; and

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

7. A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

11. A computer program product for identifying a message as suspicious, the computer program product being embodied in a non-transitory computer readable storage medium and comprising computer instructions for:

extracting from a received email message a sender of the received message, wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

12. A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

25. The method of claim 1, further comprising placing the received email message in a spam inbox, when the received email message is identified as suspicious.

26. The method of claim 1, further comprising preventing execution of content contained in the received email message, when the received email message is identified as suspicious.

27. The method of claim 1, further comprising presenting a warning that describes a circumstance associated with the identification of the received email message as suspicious.

IX. EVIDENCE APPENDIX

Not Applicable.

X. RELATED PROCEEDINGS APPENDIX

Not Applicable.

Respectfully submitted,

Dated: February 7, 2012

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

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	310	310
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**310**

Electronic Acknowledgement Receipt

EFS ID:	12012990
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	07-FEB-2012
Filing Date:	27-SEP-2005
Time Stamp:	02:44:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$310
RAM confirmation Number	7816
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-036-appeal-brief.pdf	187983 988b0b7a91855ad6a26b2720197d62e5299bce2e	no	14
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29696 0c69a37d7d44896245a66d16b5d7120515fb40eb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	217679		

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.

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

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 - 4 months with $0 paid	2254	1	990	990

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**990**

Electronic Acknowledgement Receipt

EFS ID:	12012994
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	07-FEB-2012
Filing Date:	27-SEP-2005
Time Stamp:	02:49:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$990
RAM confirmation Number	7820
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	Fee Worksheet (SB06)	fee-info.pdf	29950 e7f3e19d2eba0db37c20403f35b10b5af4cd486e	no	2

Warnings:

Information:

Total Files Size (in bytes):	29950

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 08/25/2011

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	
ART UNIT	PAPER NUMBER
2476	
MAIL DATE	DELIVERY MODE
08/25/2011	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.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 11/237,004	**Applicant(s)** ROSKIND ET AL.	
	Examiner Timothy J. Weidner	**Art Unit** 2476	

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

THE REPLY FILED 07 August 2011 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *6* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

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

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

NOTICE OF APPEAL

2. ☒ The Notice of Appeal was filed on *07 August 2011*. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

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

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☒ Applicant's reply has overcome the following rejection(s): 35 USC 101.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-3,6-8,11-13 and 25-27 under 35 USC 103 as set forth in the office action dated 2/18/11*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2476

/Timothy J Weidner/
Examiner, Art Unit 2476

Receipt date: 08/07/2011
OK TO ENTER: /T.W./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: August 7, 2011.

/Aaron T. Emigh/
Aaron Emigh

AMENDMENT B (AFTER FINAL)

UNDER 37 CFR 1.116

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

Dear Sir:

This is in response to the Office Action mailed February 18, 2011. The following amendments and remarks are respectfully submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: August 7, 2011.

/Aaron T. Emigh/
Aaron Emigh

AMENDMENT B (AFTER FINAL)

UNDER 37 CFR 1.116

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

Dear Sir:

This is in response to the Office Action mailed February 18, 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. (previously presented) A method for identifying a message as suspicious, comprising:

extracting from a received email message a sender of the received message, wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

2. (original) A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. (original) A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

4. (canceled)

5. (canceled)

6. (previously presented) A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received email message a sender of the received message, wherein the sender is an email address;

determine a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determine whether the first source IP address and the second source IP address are associated with the same geographical region; and

identify the received message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region; and

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

7. (original) A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. (original) A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

9. (canceled)

10. (canceled)

11. (currently amended) A computer program product for identifying a message as suspicious, the computer program product being embodied in a non-transitory computer readable storage medium and comprising computer instructions for:

extracting from a received email message a sender of the received message, wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

12. (original) A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. (original) A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

14-24. (canceled)

25. (previously presented) The method of claim 1, further comprising placing the received email message in a spam inbox, when the received email message is identified as suspicious.

26. (previously presented) The method of claim 1, further comprising preventing execution of content contained in the received email message, when the received email message is identified as suspicious.

27. (previously presented) The method of claim 1, further comprising presenting a warning that describes a circumstance associated with the identification of the received email message as suspicious.

28-30. (canceled)

REMARKS

Claims 1-3, 6-8, 11-13, and 25-27 are pending. Claim 11 has been amended in order to present it in better form for consideration on appeal. Support for the amendment can be found without limitation at paragraph 29 of the specification.

The Examiner has rejected claim 11 under 35 USC 101 as being directed to non-statutory subject matter. The Examiner stated in the Final Office Action to which this Amendment is responsive that "[claim 11] may be amended to narrow the claim to cover only statutory embodiments…by adding the limitation 'non-transitory' to the claim" Although Applicant believes that claim 11 is already directed to statutory subject matter, in order to reduce the issues in controversy, Applicant is amending claim 11 as suggested by the Examiner.

Applicant respectfully requests that the amendment be entered in order to present the rejected claims in better form for consideration on appeal. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: August 7, 2011

/Aaron T. Emigh/
Aaron Emigh

Customer #85853
Aaron Emigh
762 Judith Court
Incline Village, NV 89451
Tel. 415-297-1305

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: August 7, 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-036).

Respectfully submitted,

Dated: August 7, 2011

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

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:	10682239
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	07-AUG-2011
Filing Date:	27-SEP-2005
Time Stamp:	21:30:53
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	6329
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-036-amendment-d-appeal-notice.pdf	86433 015e86482a056acbe8d159894e200dab82683d66	yes	6

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment After Final	1	1
Claims	2	4
Applicant Arguments/Remarks Made in an Amendment	5	5
Notice of Appeal Filed	6	6

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	31661 071431472635277a3b721a51e354b319162119d5	no	2

Warnings:

Information:

Total Files Size (in bytes):	118094

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
11/237,004	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 08/07/2011	(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))	* 12	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 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 ($)	ADDITIONAL FEE ($)	OR	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:
/STEFANIE BRYCE/

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 02/18/2011

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	
ART UNIT	PAPER NUMBER
2476	
MAIL DATE	DELIVERY MODE
02/18/2011	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)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2476	

-- 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 *03 December 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) *1-3,6-8,11-13,16 and 18-30* is/are pending in the application.

4a) Of the above claim(s) *16,18-24 and 28-30* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-8,11-13 and 25-27* 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

Response to Amendment

Claims 1, 6, 11, and 16 have been amended.

Claims 5, 10, and 15 have been cancelled.

Claims 25-30 are new.

Claims 1-3, 6-8, 11-13, 16, and 18-30 are pending.

Response to Arguments

In response to arguments/amendments filed 12/3/2010:

Arguments/amendments, page 6, regarding claims 1-3, 5, 16, and 18-24 rejected under 35 USC 101 are considered sufficient to overcome the rejections. Therefore, the rejections are withdrawn.

Arguments/amendments, page 6, regarding claims 11-13 and 15 rejected under 35 USC 101, have been considered but they are not persuasive. Arguments appear to address a rationale not applied in the rejection of said claims, and they do not address the rationale provided in the rejection. Therefore, the rejections are maintained. See MPEP 714.03 ("Where an amendment substantially responds to the rejections, objections, or requirements in a non-final Office action (and is a bona fide attempt to advance the application to final action) but contains a minor deficiency (e.g., fails to treat every rejection, objection, or requirement), the examiner may simply act on the amendment and issue a new (non-final or final) Office action. The new Office action may simply reiterate the rejection, objection, or requirement not addressed by the amendment").

Arguments/amendments, pages 7-11, regarding claims rejected under 35 USC 103, have been considered but are moot in view of the new ground(s) of rejection.

Election/Restrictions

Newly submitted claims 16, 18-24, and 28-30 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons:

Invention !: Claims 1-3, 6-8, 11-13, and 25-27 are drawn to packet filtering classified in class 726, subclass 13.

Invention II: Claim 16, 18-24, and 28-30 are drawn to virus detection, classified in class 726, subclass 24.

The inventions are distinct, each from the other because of the following reasons: Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, subcombination I has separate utility such as spam filtering. See MPEP § 806.05(d).

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 16, 18-24, and 28-30 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Claim Rejections - 35 USC § 101

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 11-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 11-13 are directed to "computer program product … embodied in a computer readable storage medium", which may be interpreted with the broadest reasonable interpretation to include signals. *See* MPEP 2111.01. Signals per se are 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). A claim drawn to such a computer readable medium that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "non-transitory" to the claim. *Cf Animals - Patentability,* 1077 *Off. Gaz. Pat. Office* 24 (April 21, 1987) (suggesting that applicants add the limitation "non-human" to a claim covering a multicellular organism to avoid a rejection under 35 U.S.C. § 101). Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes non-transitory embodiments and transitory signals per se. *Subject Matter Eligibility of Computer Readable Media,* 1351 OG 212 (February 23, 2010).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 3, 6, 8, 11, 13, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bandini et al. (US 2002/0199095 A1) in view of Sobel et al. (US 7366919 B1).

Regarding claim 1, Bandini teaches a method for identifying a message as suspicious (limitations in the preamble are not given patentable weight unless referred to in the body of the claim and addressed below, see MPEP 2111.02), comprising:

extracting from a received email message a sender of the received message, wherein the sender is an email address (paragraph 27, "the sender address of the incoming e-mail message is compared to …");

determining current routing data associated with the received email address, wherein the current routing data includes a first source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of incoming message is treated as first source IP address);

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP

address of SPAM is treated as second source IP address; paragraph 22, SPAM database treated as spam inbox);

determining whether the first source IP address and the second source IP address match (paragraph 32, “a match of the IP address or internet domain would enhance a finding of likely SPAM”);

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address match (paragraph 32, “a match of the IP address or internet domain would enhance a finding of likely SPAM”).

Bandini may not explicitly teach, but Sobel, which is in the same field of endeavor, teaches:

determining whether the first source IP address and the second source IP address are associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If the actual geo-location obtained in step 12 matches one of these resolved locations ..." where a match is treated as association with the same geographical region; column 5, lines 15-20, where the addresses are source IP addresses); and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If, on the other hand, the actual geo-location obtained from step 12 does not match one of these resolved locations, a declaration is made at step 16 that e-

mail 24 contains suspected spam" where not matching is treated as not associated with the same geographical region).

The purpose of Sobel is to reduce the amount of spam to which a computer is subjected (column 1, lines 6-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Bandini, e.g. have "determining … and identifying …" as claimed, to reduce the amount of spam to which a computer is subjected.

Regarding claim 3, Bandini teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 24, "fields of the record preferably correspond to the message header fields").

Regarding claim 6, Bandini teaches a system for identifying a message as suspicious (limitations in the preamble are not given patentable weight unless referred to in the body of the claim and addressed below, see MPEP 2111.02), comprising:

a processor (paragraph 11) configured to:

extract from a received email message a sender of the received message, wherein the sender is an email address (paragraph 27, "the sender address of the incoming e-mail message is compared to …");

determine current routing data associated with the received email address, wherein the current routing data includes a first source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of incoming message is treated as first source IP address);

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address (paragraph 32, “the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message” where IP address of SPAM is treated as second source IP address; paragraph 22, SPAM database treated as spam inbox);

determine whether the first source IP address and the second source IP address match (paragraph 32, “a match of the IP address or internet domain would enhance a finding of likely SPAM”);

identify the received email message as suspicious if it is determined that the first source IP address and the second source IP address match (paragraph 32, “a match of the IP address or internet domain would enhance a finding of likely SPAM”).

Bandini may not explicitly teach, but Sobel, which is in the same field of endeavor, teaches:

determine whether the first source IP address and the second source IP address are associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If the actual geo-location obtained in step 12 matches one of these resolved locations ..." where a match is treated as association with the same geographical region; column 5, lines 15-20, where the addresses are source IP addresses); and

identify the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If, on the other hand, the actual geo-location obtained from step 12 does not match one of these resolved locations, a declaration is made at step 16 that e-mail 24 contains suspected spam” where not matching is treated as not associated with the same geographical region).

The purpose of Sobel is to reduce the amount of spam to which a computer is subjected (column 1, lines 6-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Bandini, e.g. have “determine … and identify …” as claimed, to reduce the amount of spam to which a computer is subjected.

Regarding claim 8, Bandini teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 24, “fields of the record preferably correspond to the message header fields").

Regarding claim 11, Bandini teaches a computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable storage medium and comprising computer instructions (paragraph 11) (limitations in the preamble are not given patentable weight unless referred to in the body of the claim and addressed below, see MPEP 2111.02) for:

extracting from a received email message a sender of the received message, wherein the sender is an email address (paragraph 27, "the sender address of the incoming e-mail message is compared to …");

determining current routing data associated with the received email address, wherein the current routing data includes a first source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of incoming message is treated as first source IP address);

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address (paragraph 32, "the Internet Protocol (IP) address or internet domain from which a SPAM message was received is compared to the IP address or internet domains for the incoming message" where IP address of SPAM is treated as second source IP address; paragraph 22, SPAM database treated as spam inbox);

determining whether the first source IP address and the second source IP address match (paragraph 32, "a match of the IP address or internet domain would enhance a finding of likely SPAM");

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address match (paragraph 32, "a match of the IP address or internet domain would enhance a finding of likely SPAM").

Bandini may not explicitly teach, but Sobel, which is in the same field of endeavor, teaches:

determining whether the first source IP address and the second source IP address are associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If the actual geo-location obtained in step 12 matches one of these resolved locations ..." where a match is treated as association with the same geographical region; column 5, lines 15-20, where the addresses are source IP addresses); and

identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region (column 5, line 59 - column 6, line 1, “address 22 is resolved into a location … If, on the other hand, the actual geo-location obtained from step 12 does not match one of these resolved locations, a declaration is made at step 16 that e-mail 24 contains suspected spam” where not matching is treated as not associated with the same geographical region).

The purpose of Sobel is to reduce the amount of spam to which a computer is subjected (column 1, lines 6-7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Bandini, e.g. have “determining … and identifying …” as claimed, to reduce the amount of spam to which a computer is subjected.

Regarding claim 13, Bandini teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 24, “fields of the record preferably correspond to the message header fields").

Regarding claim 25, Bandini teaches placing the received email message in a spam inbox, when the received email message is identified as suspicious (paragraph 19, “quarantine the e-mail in the local message store database” where database is treated as spam inbox).

Regarding claim 26, Bandini teaches preventing execution of content contained in the received email message, when the received email message is identified as suspicious (paragraph 19, “quarantine the e-mail in the local message store database” where quarantine is treated as preventing execution of content; paragraph 31, where quarantined message including URL is treated as content not executed).

Regarding claim 27, Bandini teaches presenting a warning that describes a circumstance associated with the identification of the received email message as suspicious (paragraph 19, “generate a special message to the intended recipient indicating that the e-mail message has been diverted”).

Claims 2, 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bandini et al. (US 2002/0199095 A1) in view of Sobel et al. (US 7366919 B1), as applied to claims 1, 6, and 11 respectively above, and further in view of Kirsch (US 2005/0198159 A1).

Regarding claims 2, 7, and 12, Bandini may not explicitly teach, but Kirsch, which is in the same field of endeavor, teaches processing the received message normally if it

is determined that no prior routing data associated with the sender is available (figure 2, steps 102, 106, 114, 104 in sequence and associated text, where determining sender is not on whitelist or blacklist is treated as determining no prior routing data associated with the sender is available, and sending the email to the recipient is treated as processing the message normally).

The purpose of Kirsch is to more effectively filter unwanted e-mails (paragraph 9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kirsch with Bandini and Sobel, e.g. have "processing the received message normally if it is determined that no prior routing data associated with the sender is available" as claimed, to more effectively filter unwanted e-mails.

Conclusion

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

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Timothy J. Weidner whose telephone number is (571) 270-1825. The examiner can normally be reached on Monday - Friday, 9:00 AM - 6:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2476

/Timothy J Weidner/
Examiner, Art Unit 2476

Notice of References Cited	Application/Control No. 11/237,004	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2476	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2010/0205672 A1	08-2010	Milliken et al.	726/24
*	B	US-7,822,977 B2	10-2010	Katsikas, Peter L.	713/162
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	Timothy J Weidner	2476

✓	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	09/29/2008	07/07/2009	05/28/2010	02/15/2011					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	-	-	-					
	5	✓	✓	✓	-					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	-	-	-					
	10	✓	✓	✓	-					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	-	-	-					
	15	✓	✓	✓	-					
	16	✓	✓	✓	N					
	17	✓	-	-	-					
	18		✓	✓	N					
	19		✓	✓	N					
	20		✓	✓	N					
	21		✓	✓	N					
	22		✓	✓	N					
	23		✓	✓	N					
	24		✓	✓	N					
	25				✓					
	26				✓					
	27				✓					
	28				N					
	29				N					
	30				N					

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J Weidner	2476

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
eDAN inventorship search	9/25/2008	TJW
EAST search class/sub 370/252,389,401 713/153,154 726/22,26,27 using keywords	9/29/2008	TJW
eDAN and EAST searches above updated	7/7/2009	TJW
EAST keyword search	7/7/2009	TJW
eDAN and EAST searches above updated	5/28/2010	TJW
EAST keyword search	5/28/2010	TJW
eDAN and EAST searches above updated	2/15/2011	TJW
EAST keyword search	2/15/2011	TJW

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S122	2	"20020199095".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S123	22	("20020010800" | "20030014665" | "20030126468" | "20040078485" | "20040146006" | "20050213570" | "20050074001" | "20060029104" | "6851028" | "7299296" | "7328451").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S124	7708	370/252.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S125	4024	S124 and address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S126	1565	S124 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S127	367	S124 and IP adj address with (compar$4 differen$5 match $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S128	4498	S124 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

S129	207	S128 and S127	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S130	91	S129 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S131	936	sender near id and (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S132	377	sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S133	0	S124 and S132	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S134	390	713/154.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S135	2	S131 and S134	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S136	1557	713/153.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S137	8	S131 and S136	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

S138	0	S131 and IP near spoof$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S139	210	S134 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S140	105	S139 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S141	92	S140 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S142	326	S131 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S143	146	S132 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S144	71	S143 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S145	0	S127 and S131	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S146	2	"20070014276".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

S147	2	"20030035370".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S148	42	"726".clas. and sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S149	335	(sender near id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S150	195	S149 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S151	12	"370".clas. and S150	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S152	33	"713".clas. and S150 not S151	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S153	14	"726".clas. and S150 not (S151 S152)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S154	136	S150 not (S151 S152 S153)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S155	5	(mailfrom mail adj from) and (email e adj mail instant near message) and (IP adj address) not S154	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

S156	2537	726/22.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S157	489	S156 and (email e adj mail instant near messag$3) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S158	101	S156 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S159	76	S158 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S160	3361	726/26.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S161	2363	726/27.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S162	7971	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S163	38	S160 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S164	34	S163 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

S165	12	S161 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S166	9	S165 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S167	170	S162 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S168	1	S162 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S169	2	S162 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S170	10206	370/401.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S171	1	S170 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S172	255	S170 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S173	185	S172 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

S174	225	S170 and (email e adj mail instant near messag$3) same ((IP adj address) (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S175	8	S170 and (email e adj mail instant near messag$3) same ((IP adj address) and (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S176	311	(filter$3 with (email e?mail (e adj mail))) and (ip with match $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S177	211	S176 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S178	48	S177 and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S179	35	(US-20040078485-$ or US-20020010800-$ or US-20030014665-$ or US-20040146006-$ or US-20060029104-$ or US-20030126468-$ or US-20050074001-$ or US-20050213570-$ or US-20040100972-$ or US-20050018618-$ or US-20030152035-$ or US-20040181694-$ or US-20040205135-$ or US-20070217408-$ or US-20040260778-$ or US-20030131063-$ or US-20070112966-$ or US-20050198159-$ or US-20010040697-$ or US-20040054924-$ or US-20070297408-$ or US-20030043853-$ or US-20050081059-$ or US-20050108573-$ or US-20050204159-$ or US-20050216770-$).did. or (US-	US-PGPUB; USPAT	OR	ON	2011/02/14 18:26

		20020199095-$).did. or (US-7299296-$ or US-6851028-$ or US-7413085-$ or US-7207062-$ or US-7366919-$ or US-7290035-$ or US-7360086-$ or US-7117358-$).did.				
S180	2	S179 and inbox	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S181	89	inbox with compar$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S182	45	S181 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S183	188	inbox with match$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S184	121	S183 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26
S185	110	S184 not S182	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/02/14 18:26

2/15/2011 2:15:13 PM
C:\Documents and Settings\tweidner\My Documents\EAST\Workspaces\11237004.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: December 3, 2010.

/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 June 3, 2010. 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 identifying a message as suspicious, comprising:

extracting from a received email message a sender of the received message[[;]], wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received email message as suspicious if ~~the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message~~ it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

2. (original) A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. (original) A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

4. (canceled)

5. (canceled)

6. (currently amended) A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received email message a sender of the received message[[;]], wherein the sender is an email address;

determine a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determine whether the first source IP address and the second source IP address are associated with the same geographical region; and

identify the received message as suspicious if ~~the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message~~ it is determined that the first source IP address and the second source IP address are not associated with the same geographical region; and

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

7. (original) A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. (original) A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

9. (canceled)

10. (canceled)

11. (currently amended) A computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

extracting from a received email message a sender of the received message[[;]], wherein the sender is an email address;

determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address;

determining whether the first source IP address and the second source IP address are associated with the same geographical region; and

identifying the received message as suspicious if ~~the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message~~ it is determined that the first source IP address and the second source IP address are not associated with the same geographical region.

12. (original) A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. (original) A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

14. (canceled)

15. (canceled)

16. (currently amended) A method for reporting a malicious network communication, comprising:

determining that a received network communication is ~~associated with an infection~~ classified by antivirus software as infected;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information;

sending a notification that the received network communication was ~~associated with an infection~~ classified as infected, if it is determined that the first routing information and the second routing information match.

17. (canceled)

18. (previously presented) The method of claim 16, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

19. (previously presented) The method of claim 16, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the

prior network communication and wherein the third party is not a sender of the received network communication.

20. (previously presented) The method of claim 16, wherein the first routing information is associated with an IP address.

21. (previously presented) The method of claim 16, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

22. (previously presented) The method of claim 16, wherein the received network communication is associated with email.

23. (previously presented) The method of claim 16, wherein the received network communication is associated with an instant message.

24. (previously presented) The method of claim 16, wherein the prior network communication is associated with email.

25. (new) The method of claim 1, further comprising placing the received email message in a spam inbox, when the received email message is identified as suspicious.

26. (new) The method of claim 1, further comprising preventing execution of content contained in the received email message, when the received email message is identified as suspicious.

27. (new) The method of claim 1, further comprising presenting a warning that describes a circumstance associated with the identification of the received email message as suspicious.

28. (new) The method of claim 16, wherein the network communication is classified as infected because it includes a virus.

29. (new) The method of claim 16, wherein the network communication is classified as infected because it includes a worm.

30. (new) The method of claim 16, wherein the network communication is classified as infected because it includes a Trojan horse.

REMARKS

Claims 1-3, 6-8, 11-13, 16, and 18-30 are pending. Claims 5, 10, and 15 have been canceled. New claims 25-30 have been added. Claims 1, 6, 11, and 16 have been amended. Support for the amendments can be found without limitation at paragraphs 32, 56, and 57, and Figures 18 and 19A, of the specification.

The Examiner has rejected claims 1-3, 5, 11-13, 15, 16, and 18-24 under 35 USC 101 as being directed to non-statutory subject matter on the basis that "a statutory 'process' under 35 USC 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of in re Bilski 88 USPQ2d 1385." Applicant respectfully traverses. The Appellate Court decision to which the Examiner refers has been overturned by the Supreme Court, and the *per se* machine-or-transformation test that forms the basis of the Examiner's rejection has been explicitly disavowed. ("The machine-or-transformation test is not the sole test for patent eligibility under § 101. The Court's precedents establish that although that test may be a useful and important clue or investigative tool, it is not the sole test for deciding whether an invention is a patent-eligible process under § 101." *Bilski v. Kappos*, No. 08-964, 561 U.S. ____ Slip Opinion, June 28, 2010.) Therefore, according to the Supreme Court, the Examiner erred in applying a strict machine-or-transformation test. Rather, the germane question is whether the claims recite an abstract idea rather than a statutory method. They do not: such recited limitations as "extracting from a received email message a sender of the received message" or "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox," as recited in independent claims 1, 6, and 11, and "extracting first routing information from the received network communication" or "sending a notification that the received network communication was associated with an infection," as recited in independent claim 16, are actions and are not mere ideas.

Claims 1, 6, 11, and 16 are therefore believed to be allowable.

Claims 2, 3, and 5 depend from claim 1 and are believed to be allowable for the reasons described above.

Claims 7, 8, and 10 depend from claim 6 and are believed to be allowable for the reasons described above.

Claims 12, 13, and 15 depend from claim 11 and are believed to be allowable for the reasons described above.

Claims 18-24 depend from claim 16 and are believed to be allowable for the reasons described above.

The Examiner has rejected claims 1-3, 6-8, 11-13, 16, 18-20, 22, and 24 under 35 USC 103(a) as being unpatentable over Doyle et al (US 2003/0043853 A1), hereinafter referred to as Doyle, in view of Bandini et al (US 2002/0199095 A1), hereinafter referred to as Bandini, further in view of Kirsch (US 2005/0198159 A1).

Neither Doyle, Bandini, nor Kirsch, alone or in combination, appear to teach or suggest "determining a current routing data associated with the received email address, wherein the current routing data includes a first source IP address; retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox and wherein the prior routing data includes a second source IP address; determining whether the first source IP address and the second source IP address are associated with the same geographical region; and identifying the received email message as suspicious if it is determined that the first source IP address and the second source IP address are not associated with the same geographical region," as recited in amended independent claims 1 and 11, and similarly in amended independent claim 6.

Amended independent claims 1, 6, and 11 contain subject matter similar to that previously presented in claims 5, 10, and 15 (now canceled). With regard to those claims, the Examiner rejected them under 35 USC 103(a) as unpatentable over Doyle in view of Bandini, further in view of Kirsch, and further in view of Sobel et al (US 7,366,919 B1), hereinafter referred to as Sobel. Accordingly, since the Examiner has acknowledged that Doyle, Bandini and Kirsch do not teach the added limitations, Applicant will treat these claims herein as if rejected on that basis.

First, Bandini not only appears not to teach "wherein the prior email message is in an inbox," but in fact appears to teach away from this, in that Bandini teaches comparing email to

spam email in a spam database ("The email relay compares attributes of the messages to data received from SPAM messages, which is stored in a SPAM database," Bandini, Abstract). This is fundamentally different than the technique claimed in the instant application, which involves comparing an email to previously received emails in an inbox, e.g. which are *not* spam, to determine whether the routing of the email was suspicious. Therefore, Bandini cannot be combined with Doyle, Kirsch and Sobel to achieve the result postulated by the Examiner.

Second, the combination of Doyle, Bandini, Kirsch, and Sobel is not obvious.

Merely finding the claimed elements in a disparate assortment of prior art references is not adequate to show obviousness. As *KSR* articulates, "Inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known." *KSR* goes on to say that "A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post reasoning. See *Graham*, 383 U. S., at 36 (warning against a 'temptation to read into the prior art the teachings of the invention in issue' and instructing courts to 'guard against slipping into the use of hindsight' (quoting *Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964)))."

The Examiner has proposed a combination of Doyle, Bandini, Kirsch, and Sobel in a manner that, if it would work as envisioned by the Examiner (which it would not), would create an unexpected result that solves a long-felt problem. This indicates that the combination is non-obvious, and that the process used to construct the obviousness argument was a hindsight-driven reconstruction gleaned only from Appellant's disclosure, and not from a process that one skilled in the art would reasonably undertake. This conflicts with the teachings of *In re McLaughlin* 443 F.2d 1392, 1395, 170 USPQ 209, 212 (CCPA 1971): "Any judgment on obviousness is in a sense necessarily a reconstruction based on hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill in the art at the time the claimed invention was made and **does not include knowledge gleaned only from applicant's disclosure**, such a reconstruction is proper." (Emphasis added.)

Applicant believes that the Examiner's reconstruction is based on improper hindsight and includes knowledge gleaned only from Appellant's disclosure. The combination yields unexpected results that are greater than an expected combination of the constituent parts that

transcend a mere addition of their respective functionality (for example, by learning from legitimate emails from a sender and detecting a spoofed email coming from an MTA that is far from a legitimate MTA, e.g. in Eastern Europe, while allowing variation amongst IP addresses of MTAs that may interchangeably send legitimate email from the sender).

Amended independent claims 1, 6, and 11 are therefore believed to be allowable.

Claims 2 and 3 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claims 7 and 8 depend from claim 6 and are believed to be allowable for the same reasons described above.

Claims 12 and 13 depend from claim 11 and are believed to be allowable for the same reasons described above.

Neither Doyle, Bandini, nor Kirsch alone or in combination, appear to teach or suggest "determining that a received network communication is classified by antivirus software as infected," as recited in amended independent claim 16.

Additionally, neither Doyle, Bandini, nor Kirsch, alone or in combination, appear to teach or suggest "sending a notification that the received network communication was classified as infected, if it is determined that the first routing information and the second routing information match," as recited in independent claim 16. Since there is no teaching or suggestion of classification as infectious, there cannot be any action predicated on such a classification.

Independent claim 16 is therefore believed to be allowable.

Claims 18-20, 22, and 24 depend from claim 16 and are believed to be allowable for the same reasons described above.

The Examiner has rejected claims 5, 10, 15, and 21 under 35 USC 103(a) as being unpatentable over Doyle in view of Bandini, further in view of Kirsch, and further in view of Sobel et al (US 7,366,919 B1), hereinafter referred to as Sobel.

Claims 5, 10, and 15 have been canceled.

Neither Doyle, Bandini, Kirsch, nor Sobel, alone or in combination, appear to teach or suggest either "determining that a received network communication is classified by antivirus software as infected," or "sending a notification that the received network communication was classified as infected, if it is determined that the first routing information and the second routing information match," as recited in amended independent claim 16.

Additionally, as described above, the combination of Doyle, Bandini, Kirsch, and Sobel, even if they could be combined to perform the method of claim 16 (which they cannot), is not obvious.

Amended independent claim 16 is therefore believed to be allowable.

Claim 21 depends from claim 16 and is believed to be allowable for the same reasons described above.

The Examiner has rejected claim 23 under 35 USC 103(a) as being unpatentable over Doyle in view of Bandini, further in view of Kirsch, and further in view of Banister et al (US 2004/0260768 A1).

Neither Doyle, Bandini, Kirsch, nor Banister, alone or in combination, appear to teach or suggest either "determining that a received network communication is classified by antivirus software as infected," or "sending a notification that the received network communication was classified as infected, if it is determined that the first routing information and the second routing information match," as recited in amended independent claim 16.

Additionally, the combination of Doyle, Bandini, Kirsch, and Banister, even if they could be combined to perform the method of claim 16 (which they cannot), is not obvious.

Amended independent claim 16 is therefore believed to be allowable.

Claim 23 depends from claim 16 and is believed to be allowable for the same reasons described above.

New claims 25-27 depend from claim 1 and are believed to be allowable for the same reasons described above.

New claims 28-30 depend from claim 16 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: December 3, 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.

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-036).

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

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 - 3 months with $0 paid	2253	1	555	555
Miscellaneous:				
			Total in USD ($)	**633**

Electronic Acknowledgement Receipt

EFS ID:	8967946
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	03-DEC-2010
Filing Date:	27-SEP-2005
Time Stamp:	22:55:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$633
RAM confirmation Number	7923
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-036-amendment-c.pdf	142969 6f0f3255b4fd6ba116e8ceb2bf51d0e5208e2a4e	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	31701 4e8478f63c2eed0d9369f0d80018857b7cb08d39	no	2

Warnings:

Information:

Total Files Size (in bytes):	174670

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
11/237,004	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 12/03/2010	(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))	* 4	Minus	***4	= 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:
/BURNELL L. ROSS/

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 06/03/2010

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	
ART UNIT	PAPER NUMBER
2476	
MAIL DATE	DELIVERY MODE
06/03/2010	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)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2476	

-- 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 *11 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) *1-3,5-8,10-13,15,16 and 18-24* is/are pending in the application.

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

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-8,10-13,15,16 and 18-24* is/are rejected.

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

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

Application Papers

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

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

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 11, 2010 has been entered.

Response to Amendment

Claims 1, 6, 11, and 16 are currently amended.

Claims 1-3, 5-8, 10-13, 15, 16, and 18-24 are pending.

Response to Arguments

In response to applicant's arguments/amendments filed January 11, 2010:

Regarding objections to the claims, arguments/amendments have been considered and are persuasive. The objections are withdrawn.

Regarding claims 11-15 rejected under 35 USC 101, arguments/amendments have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 1-3, 5-8, 10-13, 15, 16, and 18-24 rejected under 35 USC 103, arguments/amendments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-3, 5, 11-13, 15, 16, and 18-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-3, 5, 16, and 18-24 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method steps involve analyzing and comparing email messages in an inbox, which can be performed mentally.

Claims 11-13 and 15 are directed to "computer program product … embodied in a computer readable storage medium", which may be interpreted with the broadest reasonable interpretation to include signals. *See* MPEP 2111.01. Signals per se are 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). A claim drawn to such a computer readable medium that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "non-

transitory" to the claim. *Cf Animals - Patentability,* 1077 *Off. Gaz. Pat. Office* 24 (April 21, 1987) (suggesting that applicants add the limitation "non-human" to a claim covering a multicellular organism to avoid a rejection under 35 U.S.C. § 101). Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes non-transitory embodiments and transitory signals per se. *Subject Matter Eligibility of Computer Readable Media,* 1351 OG 212 (February 23, 2010).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-3, 6-8, 11-13, 16, 18-20, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) in view of Bandini et al. (US 2002/0199095 A1) and Kirsch (US 2005/0198159 A1).

Regarding claims 1, 6, and 11, Doyle teaches a method, system, and computer program product being embodied in a computer readable storage medium and comprising computer instructions (paragraphs 32-33, processor and memory together perform the steps of the method), for identifying a message as suspicious (limitations in the preamble are not given patentable weight unless they are referred to the body of the claim and addressed below, see MPEP 2111.02), comprising:

extracting from a received message a sender of the received message (paragraph 69, lines 1-7, a MAC address is an identity of a sender);

retrieving prior routing data (paragraph 71, lines 12-14, an IP address is prior routing data) associated with a prior message received previously from the sender (paragraphs 69, lines 5-6); and

identifying the received message as suspicious/infectious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicated the received message was received from a different originating source than the prior message (paragraph 71, lines 17-20; discards the packet if there are different source IP addresses).

Doyle may not explicitly teach the message includes email and a sender is an email address. Bandini, which is in the same field of endeavor, teaches comparison of current and prior email addresses (paragraph 19) including attributes such as sender address and matching IP address (paragraphs 26 and 32) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. have the message include email and a sender is an email address, to reduce the number of spam messages received by users.

Doyle and Bandini may not explicitly teach, but Kirsch, which is in the same field of endeavor, teaches the prior email message is in an inbox (paragraph 24, “folders of saved messages may also be checked to construct the whitelist”; paragraph 58, “the whitelist is constructed as above ... messages in the e-mail program's "Inbox" ... are analyzed ... to see if any are messages from a sender (or site) on the whitelist") for the

purpose of filtering unwanted e-mails based on sender information (paragraph 9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kirsch with Doyle and Bandini, e.g. have the prior email message is in an inbox, to filter unwanted e-mails based on sender information.

Regarding claims 2, 7, and 12, Doyle teaches processing the received message normally if it is determined that no prior routing data associated with the sender is available (paragraph 69, lines 1-3 and 11-13).

Regarding claims 3, 8, and 13, Doyle teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 52, lines 4-6).

Regarding claim 16, Doyle teaches a method for reporting a malicious network communication (limitations in the preamble are not given patentable weight unless they are referred to the body of the claim and addressed below, see MPEP 2111.02), comprising:

determining that a received network communication is suspicious (paragraph 71, lines 17-20; different source IP addresses),

extracting first routing information from the received network communication (paragraph 71, lines 12-14).

Doyle may not explicitly teach, but Bandini, which is in the same field of endeavor, teaches:

determining whether second routing information from a prior network communication received previously matches the first routing information (paragraph 32);

sending a notification that the received network communication was suspicious (paragraph 35), if it is determined that the first routing information and the second routing information match (paragraph 32)

The purpose of Bandini is to reduce the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. have determining whether second routing information from a prior network communication received previously matches the first routing information; sending a notification that the received network communication was suspicious, if it is determined that the first routing information and the second routing information match, to reduce the number of spam messages received by users.

Doyle and Bandini may not explicitly teach, but Kirsch, which is in the same field of endeavor, teaches suspicious communications are associated with an infection (paragraph 2, "The proliferation of junk e-mail, or “spam” can be a major annoyance to email users who are bombarded by unsolicited e-mails that clog up their mailboxes” where such fits an interpretation of “infection” as detrimental colonization (major annoyance … clog up) of a host organism (mailboxes) with a foreign species (spam)) for the purpose of filtering unwanted e-mails based on sender information (paragraph 9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kirsch with Doyle and Bandini, e.g. have suspicious communications are associated with an infection, to filter unwanted e-mails based on sender information.

Regarding claim 18, Doyle may not explicitly teach sending the notification to a sender associated with the prior network communication. Bandini teaches sending the notification to a sender associated with the prior network communication (paragraph 40) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle and Kirsch, e.g. sending the notification to a sender associated with the prior network communication, to reduce the number of spam messages received by users.

Regarding claim 19, Doyle may not explicitly teach notifying a third party. Bandini teaches sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication (paragraph 35) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle and Kirsch, e.g. sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, to reduce the number of spam messages received by users.

Regarding claim 20, Doyle teaches the first routing information is associated with an IP address (paragraph 71, lines 12-20).

Regarding claims 22 and 24, Doyle may not explicitly teach email. Bandini teaches comparison of current and prior email addresses (paragraph 19) including

attributes such as sender address and matching IP address (paragraphs 26 and 32) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle and Kirsch, e.g. have the message include email and a sender is an email address, to reduce the number of spam messages received by users.

Claims 5, 10, 15, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) in view of Bandini et al. (US 2002/0199095 A1) and Kirsch (US 2005/0198159 A1) as applied to claims 1, 6, 11, and 16 respectively above, and further in view of Sobel et al. (US 7366919 B1).

Regarding claims 5, 10, 15, and 21, Doyle teaches determining a first source IP address associated with the prior message (paragraph 71, lines 12-14), and determining a second source IP address associated with the prior message (paragraph 69, lines 1-7). However, Doyle may not explicitly teach determining whether the first and second IP addresses are associated with the same geographical region.

Sobel, which is in the same field of endeavor, teaches resolving two IP addresses into geographical regions and determining whether they are the same for the purpose of detecting spam (column 5, lines 15-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Doyle, Bandini, and Kirsch, e.g. determine whether the first and second source addresses belong to the same geographical region, to detect spam.

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) in view of Bandini et al. (US 2002/0199095 A1) and Kirsch (US 2005/0198159 A1) as applied to claim 16 above, and further in view of Banister et al. (US 2004/0260778 A1).

Regarding claim 23, Doyle teaches the prior routing data includes an IP address (paragraph 71, lines 12-14), but may not explicitly teach an instant messaging session.

Banister, which is in the same field of endeavor, teaches network address verification using instant messages for the purpose of fining users for sending spam (paragraphs 50 and 56). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Banister with Doyle, Bandini, and Kirsch, e.g. have the prior routing data include an IP address retrieved from a prior instant messaging session, to fine users for sending spam.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Paul (US 5999932) teaches comparing incoming emails to a filter list “associated with” prior email header information from an inbox (column 3, lines 20-40 and column 4, lines 30-50).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Timothy J. Weidner whose telephone number is (571) 270-1825. The examiner can normally be reached on Monday - Friday, 8:00 AM - 5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2476

/Timothy J Weidner/
Examiner, Art Unit 2476

Notice of References Cited	Application/Control No. 11/237,004	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2476	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,999,932 A	12-1999	Paul, Sunil	709/206
*	B	US-2003/0110227 A1	06-2003	O'Hagan, Timothy Patrick	709/206
*	C	US-2005/0015432 A1	01-2005	Cohen, Hunter C.	709/201
*	D	US-2005/0060535 A1	03-2005	Bartas, John Alexander	713/154
*	E	US-2010/0088765 A1	04-2010	Lund et al.	726/22
	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
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	Timothy J Weidner	2476

✓	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	09/29/2008	07/07/2009	05/28/2010						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	-	-						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	-	-						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	-	-						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	-	-						
	18		✓	✓						
	19		✓	✓						
	20		✓	✓						
	21		✓	✓						
	22		✓	✓						
	23		✓	✓						
	24		✓	✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S58	2	"20020199095".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S59	22	("20020010800" | "20030014665" | "20030126468" | "20040078485" | "20040146006" | "20050213570" | "20050074001" | "20060029104" | "6851028" | "7299296" | "7328451").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S60	6394	370/252.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S61	3357	S60 and address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S62	1296	S60 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S63	293	S60 and IP adj address with (compar$4 differen$5 match $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S64	4239	S60 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50

S65	192	S64 and S63	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S66	82	S65 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S67	844	sender near id and (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S68	342	sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S69	0	S60 and S68	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S70	337	713/154.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S71	1	S67 and S70	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S72	1349	713/153.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S73	8	S67 and S72	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50

S74	0	S67 and IP near spoof$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S75	176	S70 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S76	88	S75 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S77	82	S76 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S78	280	S67 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S79	125	S68 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S80	65	S79 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S81	0	S63 and S67	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S82	2	"20070014276".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50

S83	2	"20030035370".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S84	39	"726".clas. and sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S85	288	(sender near id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S86	179	S85 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S87	12	"370".clas. and S86	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S88	29	"713".clas. and S86 not S87	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S89	12	"726".clas. and S86 not (S87 S88)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S90	126	S86 not (S87 S88 S89)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S91	5	(mailfrom mail adj from) and (email e adj mail instant near message) and (IP adj address) not S90	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50

S92	2088	726/22.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S93	395	S92 and (email e adj mail instant near messag$3) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S94	83	S92 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S95	64	S94 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S96	2747	726/26.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S97	1943	726/27.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S98	7166	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S99	31	S96 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S100	28	S99 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50

S101	9	S97 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S102	8	S101 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S103	157	S98 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S104	1	S98 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S105	2	S98 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S106	9293	370/401.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S107	1	S106 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S108	227	S106 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S109	171	S108 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50

S110	207	S106 and (email e adj mail instant near messag$3) same ((IP adj address) (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S111	8	S106 and (email e adj mail instant near messag$3) same ((IP adj address) and (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S112	286	(filter$3 with (email e?mail (e adj mail))) and (ip with match $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S113	197	S112 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S114	47	S113 and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:50
S115	35	(US-20040078485-$ or US-20020010800-$ or US-20030014665-$ or US-20040146006-$ or US-20060029104-$ or US-20030126468-$ or US-20050074001-$ or US-20050213570-$ or US-20040100972-$ or US-20050018618-$ or US-20030152035-$ or US-20040181694-$ or US-20040205135-$ or US-20070217408-$ or US-20040260778-$ or US-20030131063-$ or US-20070112966-$ or US-20050198159-$ or US-20010040697-$ or US-20040054924-$ or US-20070297408-$ or US-20030043853-$ or US-20050081059-$ or US-20050108573-$ or US-20050204159-$ or US-	US-PGPUB; USPAT	OR	ON	2010/05/27 09:58

		20050216770-$).did. or (US-20020199095-$).did. or (US-7299296-$ or US-6851028-$ or US-7413085-$ or US-7207062-$ or US-7366919-$ or US-7290035-$ or US-7360086-$ or US-7117358-$).did.				
S116	2	S115 and inbox	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 09:58
S117	72	inbox with compar$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 10:14
S118	41	S117 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 10:14
S119	170	inbox with match$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 14:58
S120	114	S119 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 14:58
S121	104	S120 not S118	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/05/27 14:58

EAST Search History (Interference)

< This search history is empty>

5/ 28/ 2010 12:51:16 PM
C:\ Documents and Settings\ tweidner\ My Documents\ EAST\ Workspaces\ 11237004.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J Weidner	2476

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
eDAN inventorship search	9/25/2008	TJW
EAST search class/sub 370/252,389,401 713/153,154 726/22,26,27 using keywords	9/29/2008	TJW
eDAN and EAST searches above updated	7/7/2009	TJW
EAST keyword search	7/7/2009	TJW
eDAN and EAST searches above updated	5/28/2010	TJW
EAST keyword search	5/28/2010	TJW

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: January 11, 2010.

/Aaron T. Emigh/
Aaron Emigh

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL FILED WITH AMENDMENT B

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

This is a Request for Continued Examination (RCE) under 37 CFR §1.114 of the above-identified application.

1. Submission required under 37 CFR §1.114

a. ☒ Enclosed:

- ☒ Amendment/Reply
- ☐ Affidavit(s)/Declaration(s)
- ☐ Information Disclosure Statement (IDS)
- ☐ Other

Respectfully submitted,

Dated: January 11, 2010

/Aaron T. Emigh/
Aaron Emigh
Customer #85853

Electronic Patent Application Fee Transmittal

Application Number:	11237004
Filing Date:	27-Sep-2005
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Filer:	Aaron Thompson Emigh
Attorney Docket Number:	PB-036

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($)
Miscellaneous:				
Request for continued examination	2801	1	405	405
		Total in USD ($)		**960**

Electronic Acknowledgement Receipt

EFS ID:	6785635
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	11-JAN-2010
Filing Date:	27-SEP-2005
Time Stamp:	15:29:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$960
RAM confirmation Number	1803
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-036-amendment-b.pdf	141726 81ffaf74e460635616d45939993627666fbe4826	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment Submitted/Entered with Filing of CPA/RCE	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	10
	Extension of Time	11	11
	Request for Continued Examination (RCE)	12	12

Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	31848 cbd5239d5914f309db24ba4395f040a49580e1e9	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	173574	

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:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: January 11, 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 10, 2009. 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 identifying a message as suspicious, comprising:

extracting from a received email message a sender of the received message;

wherein the sender is an email address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox; and

identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message.

2. (original) A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. (original) A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

4. (canceled)

5. (previously presented) A method as recited in claim 1, wherein identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message includes:

determining a first source IP address associated with the received message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

6. (currently amended) A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received email message a sender of the received message;

wherein the sender is an email address;

retrieve a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox; and

identify the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message; and

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

7. (original) A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. (original) A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

9. (canceled)

10. (previously presented) A system as recited in claim 6, wherein the processor is configured to identify the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message at least in part by:

determining a first source IP address associated with the received message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

11. (currently amended) A computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

extracting from a received email message a sender of the received message;

wherein the sender is an email address;

retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox; and

identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message.

12. (original) A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. (original) A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

14. (canceled)

15. (previously presented) A computer program product as recited in claim 11, wherein identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message includes:

determining a first source IP address associated with the received message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

16. (currently amended) A method for reporting a malicious network communication, comprising:

determining that a received network communication is associated with an infection;

extracting first routing information from the received network communication;

determining whether second routing information from a prior network communication received previously matches the first routing information;

sending a notification that the received network communication was associated with an infection, if it is determined that the first routing information and the second routing information match.

17. (canceled)

18. (previously presented) The method of claim 16, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

19. (previously presented) The method of claim 16, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the

prior network communication and wherein the third party is not a sender of the received network communication.

20. (previously presented) The method of claim 16, wherein the first routing information is associated with an IP address.

21. (previously presented) The method of claim 16, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

22. (previously presented) The method of claim 16, wherein the received network communication is associated with email.

23. (previously presented) The method of claim 16, wherein the received network communication is associated with an instant message.

24. (previously presented) The method of claim 16, wherein the prior network communication is associated with email.

REMARKS

Claims 1-3, 5-8, 10-13, 15, 16, and 18-24 are pending. Claims 1, 6, 11, and 16 have been amended. Support for the amendments can be found without limitation at paragraph 56, and Figure 18, of the specification.

The Examiner has maintained his previous rejection of claims 11-13 and 15 under 35 USC 101 as being directed to non-statutory subject matter on the basis that "a computer program product may be solely software or signals." Claim 11 recites "a computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable **storage medium**..." (emphasis added). While acknowledging that claim 11 recites a *storage medium* (which in fact is language that was discussed in an interview on March 5, 2009 between Applicant and the Examiner, at which time the Examiner stated that he believed this language overcame his rejection), the Examiner has stated that "other recitations in the preamble are not given weight because they are not referred to in the body of the claim." Applicant respectfully traverses. The MPEP, section 2111.02, however, specifically disavows such a litmus test for whether a preamble limits a claim: "The determination of whether a preamble limits a claim is made on a case-by-case basis in light of the facts in each case; there is no litmus test defining when a preamble limits the scope of a claim. *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808, 62 USPQ2d 1781, 1785 (Fed. Cir. 2002)."

Even more specifically, MPEP 2111.02 goes on to state that "Any terminology in the preamble that limits the structure of the claimed invention must be treated as a claim limitation. See, e.g., *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257, 9 USPQ2d 1962, 1966 (Fed. Cir. 1989) (The determination of whether preamble recitations are structural limitations can be resolved only on review of the entirety of the application "to gain an understanding of what the inventors actually invented and intended to encompass by the claim."); *Pac-Tec Inc. v. Amerace Corp.*, 903 F.2d 796, 801, 14 USPQ2d 1871, 1876 (Fed. Cir. 1990) (determining that preamble language that constitutes a structural limitation is actually part of the claimed invention). See also *In re Stencel*, 828 F.2d 751, 4 USPQ2d 1071 (Fed. Cir. 1987). (The claim at issue was directed to a driver for setting a joint of a threaded collar; however, the body of the claim did not directly include the structure of the collar as part of the claimed article. The examiner did not consider the preamble, which did set forth the structure of the collar, as

limiting the claim. The court found that the collar structure could not be ignored. While the claim was not directly limited to the collar, the collar structure recited in the preamble did limit the structure of the driver. "[T]he framework - the teachings of the prior art - against which patentability is measured is not all drivers broadly, but drivers suitable for use in combination with this collar, for the claims are so limited." Id. at 1073, 828 F.2d at 754.)."

Since "computer readable storage medium" limits the structure of the invention of claim 11, it is entitled to be given weight, and the Examiner's maintenance of the rejection is improper.

Claim 11 is therefore believed to be allowable. Claims 12, 13, and 15 depend from claim 11 and are believed to be allowable for the reasons described above.

The Examiner has objected to claim 16 on the basis that the word "if" was missing. Claim 16 has been amended and is believed to be allowable.

The Examiner has rejected claims 1-3, 6-8, 11-13, 16, 18-20, 22, and 24 under 35 USC 103(a) as being unpatentable over Doyle et al (US 2003/0043853 A1), hereinafter referred to as Doyle, in view of Bandini et al (US 2002/0199095 A1), hereinafter referred to as Bandini.

Neither Doyle nor Bandini, alone or in combination, appear to teach or suggest "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox," as recited in amended independent claims 1 and 11, and similarly in amended independent claim 6.

Bandini not only appears not to teach "wherein the prior email message is in an inbox," but in fact appears to teach away from this, in that Bandini teaches comparing email to *spam* email in a spam database ("The email relay compares attributes of the messages to data received from SPAM messages, which is stored in a SPAM database," Bandini, Abstract). This is fundamentally different than the technique claimed in the instant application, which involves comparing an email to previously received emails in an inbox, e.g. which are *not* spam, to determine whether the routing of the email was suspicious.

Claims 1, 6, and 11 are therefore believed to be allowable.

Claims 2 and 3 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claims 7 and 8 depend from claim 6 and are believed to be allowable for the same reasons described above.

Claims 12 and 13 depend from claim 11 and are believed to be allowable for the same reasons described above.

Neither Doyle nor Bandini, alone or in combination, appear to teach or suggest "determining that a received network communication is associated with an infection," as recited in independent claim 16. The Examiner has acknowledged that Doyle does not teach or suggest this limitation, and has cited Bandini, paragraph 21 as teaching "suspicious communications are associated with spam infection." However, this is erroneous, as spam is not an email infection, or an infection of a host, but merely a classification applied to email. Bandini discusses spam as "unwanted messages" (Bandini, paragraph 3). There appears to be no mention of infection, and certainly no mention of "spam infection." Wikipedia's definition of "infection" (http://en.wikipedia.org/wiki/Infection, retrieved January 10, 2010) begins "An infection is the detrimental colonization of a host organism by a foreign species." Infection has become a term of art in computer security, consistent with this plain meaning of the word, referring to detrimental colonization of a host organism (i.e. a computing device) with a foreign species (i.e. a virus, worm, crimeware, malware, or other malicious software).

Additionally, neither Doyle nor Bandini, alone or in combination, appear to teach or suggest "sending a notification that the received network communication was associated with an infection, if it is determined that the first routing information and the second routing information match," as recited in independent claim 16. Since there is no teaching or suggestion of determining an infection, there cannot be any action predicated on such a determination.

This technique as claimed in the instant application is innovative because, for example, it enables users to be notified that their computers are infected, while avoiding "joe jobs" in which innocent users get inundated with false reports of infection due to email spoofing that uses their email address as a false sender. Indeed, the Examiner's rationale for combining Doyle and Bandini ("to reduce the number of spam messages received by users") is misguided, as this is not an object of the claimed technique.

Independent claim 16 is therefore believed to be allowable.

Claims 18-20, 22, and 24 depend from claim 16 and are believed to be allowable for the same reasons described above.

The Examiner has rejected claims 5, 10, 15, and 21 under 35 USC 103(a) as being unpatentable over Doyle in view of Bandini, further in view of Sobel et al (US 7,366,919 B1).

Neither Doyle, Bandini, nor Sobel, alone or in combination, appear to teach or suggest "retrieving a prior routing data associated with a prior email message received previously from the sender, wherein the prior email message is in an inbox," as recited in amended independent claims 1 and 11, and similarly in amended independent claim 6.

Claims 1, 6, and 11 are therefore believed to be allowable.

Claim 5 depends from claim 1 and is believed to be allowable for the same reasons described above.

Claim 10 depends from claim 6 and is believed to be allowable for the same reasons described above.

Claim 15 depends from claim 11 and is believed to be allowable for the same reasons described above.

Neither Doyle, Bandini, nor Sobel, alone or in combination, appear to teach or suggest "determining that a received network communication is associated with an infection," nor "sending a notification that the received network communication was associated with an infection, if it is determined that the first routing information and the second routing information match," as recited in independent claim 16.

Independent claim 16 is therefore believed to be allowable.

Claim 21 depends from claim 16 and is 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 11, 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 on 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-036).

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.: 11/237,004 Filed/Issue Date: 9/27/2005

Titled: DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

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

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

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

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

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

OR

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

1. From: 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).

☒ 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:

DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

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. 11/237004;

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

10/1/2009
Aaron T. Emigh

Radix Labs, LLC

By: 9/11/2009
James A. Roskind, Manager

Radix Labs, LLC

By: 10/1/2009
Aaron T. Emigh, Manager

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. 11/237,004, filed September 27, 2005, entitled DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS.

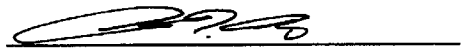
Seller hereby:

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:	6325679
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	25-OCT-2009
Filing Date:	27-SEP-2005
Time Stamp:	02:33:31
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-036-assignment-statement-1.pdf	358380 5f878ee9f3368e74f5ff6c6246865b60c34c4363	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	358380

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.: 11/237,004 Filed/Issue Date: 9/27/2005

Titled: DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

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

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

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

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

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

OR

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

1. From: _____ 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).

☒ 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.**

ASSIGNMENT OF PATENT APPLICATION

Whereas we the undersigned inventors have invented certain new and useful improvements as set forth in the patent application entitled:

DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

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. 11/237004;

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

10/1/2009
Aaron T. Emigh

Radix Labs, LLC

By: 9/11/2009
James A. Roskind, Manager

Radix Labs, LLC

By: 10/1/2009
Aaron T. Emigh, Manager

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. 11/237,004, filed September 27, 2005, entitled DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS.

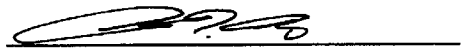
Seller hereby:

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:	6257275
Application Number:	11237004
International Application Number:	
Confirmation Number:	6024
Title of Invention:	Detecting and processing suspicious network communications
First Named Inventor/Applicant Name:	James A. Roskind
Customer Number:	85853
Filer:	Aaron Thompson Emigh
Filer Authorized By:	
Attorney Docket Number:	PB-036
Receipt Date:	14-OCT-2009
Filing Date:	27-SEP-2005
Time Stamp:	02:34:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73(b).	PB-036-assignment-statement.pdf	171880 4a53357f99d7a90e4833445cc3faf5fb63fb8fe7	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	171880

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 07/10/2009

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	
ART UNIT	PAPER NUMBER
2419	
MAIL DATE	DELIVERY MODE
07/10/2009	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)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2419	

-- 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 *09 March 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) *1-3,5-8,10-13,15,16 and 18-24* is/are pending in the application.

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

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-8,10-13,15,16 and 18-24* is/are rejected.

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

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

Application Papers

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

10)☒ The drawing(s) filed on *09 March 2009* 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

Response to Amendment

Claims 4, 9, 14, and 17 are cancelled.

Claims 1, 5, 6, 10, 11, 15, and 16 are currently amended.

Claims 18-24 are new.

Claims 1-3, 5-8, 10-13, 15, 16, and 18-24 are pending.

Response to Arguments

In response to applicant's arguments/amendments filed March 9, 2009:

Regarding objections to the drawings, abstract, specification, and rejections under 35 USC 112, arguments/amendments have been considered and are persuasive. These objections and rejections are withdrawn.

Regarding claims 11-15 rejected under 35 USC 101, arguments/amendments have been considered but are not persuasive. Claims are not directed to "computer readable storage medium," but are still directed to "computer program product." Computer program product may be solely software or signals (paragraph 29, lines 1-4). Other recitations in the preamble are not given weight because they are not referred to in the body of the claim. Therefore, the rejections are maintained.

Regarding claims 1-17 rejected under 35 USC 102 or 103, arguments/amendments have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claim 16 is objected to because of the following informalities: there appears to be a grammatical error regarding the limitation "[if] it is determined" because the word "if" appears missing. Appropriate correction is required.

Claim Rejections - 35 USC § 101

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 11-13 and 15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims are not directed to "computer readable storage medium," but instead are directed to "computer program product" which is software and signals per se (paragraph 29, lines 1-4). Software and signals do not fall into one of the four statutory categories of invention, i.e. process, machine, manufacture, or composition of matter.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-3, 6-8, 11-13, 16, 18-20, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) in view of Bandini et al. (US 2002/0199095 A1).

Regarding claims 1, 6, and 11, Doyle teaches extracting from a received message a MAC address (identity) of a sender of the received message (paragraph 69, lines 1-7), retrieving an IP address (prior routing data) (paragraph 71, lines 12-14)

associated with a prior message received previously from the sender (paragraphs 69, lines 5-6), and discarding the packet (identifying the received message as suspicious/infectuous) if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicated the received message was received from a different originating source than the prior message (paragraph 71, lines 17-20; different source IP addresses).

Further, regarding the apparatus and computer readable storage medium of claims 6 and 11, Doyle teaches a processor and memory together performs the steps of the method (paragraph 32-33).

However, Doyle may not explicitly teach the message includes email and a sender is an email address. Bandini, which is in the same field of endeavor, teaches comparison of current and prior email addresses (paragraph 19) including attributes such as sender address and matching IP address (paragraphs 26 and 32) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. have the message include email and a sender is an email address, to reduce the number of spam messages received by users.

Regarding claims 2, 7, and 12, Doyle teaches processing the received message normally if it is determined that no prior routing data associated with the sender is available (paragraph 69, lines 1-3 and 11-13).

Regarding claims 3, 8, and 13, Doyle teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 52, lines 4-6).

Regarding claim 16, Doyle teaches determining that a received network communication is suspicious (paragraph 71, lines 17-20; different source IP addresses), extracting first routing information from the received network communication (paragraph 71, lines 12-14).

However, Doyle may not explicitly teach suspicious communications are associated with an infection, and may not explicitly teach sending a notification that the received network communication was associated with an infection if it is determined that the first routing information and the second routing information match. Bandini teaches suspicious communications are associated with spam infection (paragraph 21), and sending a notification that the received network communication was associated with an infection (paragraph 35) if it is determined that first routing information and second routing information match (paragraph 32) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. associated suspicious communications with infection, and sending a notification that the received network communication was associated with an infection if it determined that the first routing information and the second routing information match, to reduce the number of spam messages received by users.

Regarding claim 18, Doyle may not explicitly teach sending the notification to a sender associated with the prior network communication. Bandini teaches sending the notification to a sender associated with the prior network communication (paragraph 40) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. sending the notification to a sender associated with the prior network communication, to reduce the number of spam messages received by users.

Regarding claim 19, Doyle may not explicitly teach notifying a third party. Bandini teaches sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication (paragraph 35) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication, to reduce the number of spam messages received by users.

Regarding claim 20, Doyle teaches the first routing information is associated with an IP address (paragraph 71, lines 12-20).

Regarding claims 22 and 24, Doyle may not explicitly teach email. Bandini teaches comparison of current and prior email addresses (paragraph 19) including

attributes such as sender address and matching IP address (paragraphs 26 and 32) for the purpose of reducing the number of spam messages received by users (paragraphs 3 and 4). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bandini with Doyle, e.g. have the message include email and a sender is an email address, to reduce the number of spam messages received by users.

Claims 5, 10, 15, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) in view of Bandini et al. (US 2002/0199095 A1) as applied to claims 1, 6, 11, and 16 respectively above, and further in view of Sobel et al. (US 7366919 B1).

Regarding claims 5, 10, 15, and 21, Doyle teaches determining a first source IP address associated with the prior message (paragraph 71, lines 12-14), and determining a second source IP address associated with the message (paragraph 69, lines 1-7). However, Doyle may not explicitly teach determining whether the first and second IP addresses are associated with the same geographical region.

Sobel, which is in the same field of endeavor, teaches resolving two IP addresses into geographical regions and determining whether they are the same for the purpose of detecting spam (column 5, lines 15-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Sobel with Doyle and Bandini, e.g. determine whether the first and second source addresses belong, to the same geographical region to detect spam.

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) in view of Bandini et al. (US 2002/0199095 A1) as applied to claim 16 above, and further in view of Banister et al. (US 2004/0260778 A1).

Regarding claim 23, Doyle teaches the prior routing data includes an IP address (paragraph 71, lines 12-14), but may not explicitly teach an instant messaging session.

Banister, which is in the same field of endeavor, teaches network address verification using instant messages for the purpose of fining users for sending spam (paragraphs 50 and 56). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Banister with Doyle and Bandini, e.g. have the prior routing data include an IP address retrieved from a prior instant messaging session, to fine users for sending spam.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bennett et al. (US 20050108573 A1) teaches a combined email sender and IP address based filtering system.

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

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Timothy J. Weidner whose telephone number is (571) 270-1825. The examiner can normally be reached on Monday - Friday, 8:00 AM - 5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Timothy J Weidner/
Examiner, Art Unit 2419

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2419

Notice of References Cited	Application/Control No. 11/237,004	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2419	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0199095 A1	12-2002	Bandini et al.	713/151
*	B	US-2005/0081059 A1	04-2005	Bandini et al.	713/201
*	C	US-2005/0108573 A1	05-2005	Bennett et al.	713/201
*	D	US-2005/0216770 A1	09-2005	Rowett et al.	713/201
*	E	US-2005/0204159 A1	09-2005	Davis et al.	713/201
*	F	US-7,117,358 B2	10-2006	Bandini et al.	713/153
	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
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	Timothy J Weidner	2419

✓	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	09/29/2008	07/07/2009							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	-							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	-							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	-							
	15	✓	✓							
	16	✓	✓							
	17	✓	-							
	18		✓							
	19		✓							
	20		✓							
	21		✓							
	22		✓							
	23		✓							
	24		✓							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	2	"20020199095".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 12:48
L8	22	("20020010800" | "20030014665" | "20030126468" | "20040078485" | "20040146006" | "20050213570" | "20050074001" | "20060029104" | "6851028" | "7299296" | "7328451"). PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L9	5303	370/252.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L10	2769	L9 and address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L11	1015	L9 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L12	233	L9 and IP adj address with (compar$4 differen$5 match $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L13	3918	L9 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L14	174	L13 and L12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L15	73	L14 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L16	743	sender near id and (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L17	297	sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L18	0	L9 and L17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L19	292	713/154.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L20	1	L16 and L19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L21	1135	713/153.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L22	7	L16 and L21	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L23	0	L16 and IP near spoof$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L24	153	L19 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L25	75	L24 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L26	70	L25 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L27	226	L16 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L28	97	L17 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L29	50	L28 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L30	0	L12 and L16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L31	2	"20070014276".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L32	2	"20030035370".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L33	29	"726".clas. and sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L34	231	(sender near id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L35	152	L34 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L36	11	"370".clas. and L35	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L37	19	"713".clas. and L35 not L36	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L38	8	"726".clas. and L35 not (L36 L37)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L39	114	L35 not (L36 L37 L38)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L40	4	(mailfrom mail adj from) and (email e adj mail instant near message) and (IP adj address) not L39	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L41	1601	726/22.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L42	304	L41 and (email e adj mail instant near messag$3) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L43	64	L41 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L44	56	L43 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L45	2158	726/26.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L46	1493	726/27.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L47	6334	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L48	24	L45 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L49	23	L48 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L50	8	L46 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L51	8	L50 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L52	139	L47 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L53	0	L47 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L54	1	L47 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L55	8269	370/401.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L56	1	L55 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L57	199	L55 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L58	157	L57 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L59	193	L55 and (email e adj mail instant near messag$3) same ((IP adj address) (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L60	8	L55 and (email e adj mail instant near messag$3) same ((IP adj address) and (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L61	249	(filter$3 with (email e?mail (e adj mail))) and (ip with match$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

L62	174	L61 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55
L63	38	L62 and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/07 13:55

EAST Search History (Interference)

<This search history is empty>

7/7/2009 2:00:22 PM
C:\Documents and Settings\tweidner\My Documents\EAST\Workspaces\11237004.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J Weidner	2419

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
eDAN inventorship search	9/25/2008	TJW
EAST search class/sub 370/252,389,401 713/153,154 726/22,26,27 using keywords	9/29/2008	TJW
eDAN and EAST searches above updated	7/7/2009	TJW
EAST keyword search	7/7/2009	TJW

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

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.
11/237,004	09/27/2005	James A. Roskind	PB-036	6024

85853 7590 03/11/2009

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
WEIDNER, TIMOTHY J	

ART UNIT	PAPER NUMBER
2419	

MAIL DATE	DELIVERY MODE
03/11/2009	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)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2419	

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

(1) *Timothy J. Weidner (Examiner)*. (3)_____.

(2) *Aaron Emigh (Inventor)*. (4)_____.

Date of Interview: *05 March 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 and 16*.

Identification of prior art discussed: *Doyle (US 2003/0043853 A1), Mastrianni (US 2002/0116641 A1)*.

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: *See Continuation Sheet*.

(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.

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2419

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

———

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

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: Discussed how 101 rejection should be withdrawn if "computer program product" were replaced with "computer readable storage medium". Discussed how 102 rejection of claim 1 might be overcome by adding limitations that specify the addresses are contained in email headers. Further, discussed how 103 rejection of claim 16 might be overcome by limiting "malicious data" to "infected". Lastly, discussed potential restriction between claims 1-15 and 16-17, and further search required in classes 713 and 726.

.

OIPE IAP78
MAR 09 2009
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

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

March 5, 2009.

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 October 6, 2008. The following amendments and remarks are respectfully submitted.

AMENDMENTS TO THE ABSTRACT

Please replace the section entitled "Abstract of the Disclosure" at page 38 with the following replacement section:

~~DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS~~

ABSTRACT OF THE DISCLOSURE

[0061] Analyzing routing information to identify and intercept unauthorized, unwanted, and/or otherwise malicious communications is disclosed. In some embodiments, routing information associated with a message currently being processed is checked against corresponding information associated with a message from the same source that was processed previously. In some embodiments, a message processing system that handled and/or otherwise has access to routing information for both messages performs the check, such as a network messaging and/or access service provider with which the sender is associated, performs the check. If the routing information for the current message does not match the corresponding information observed in the previous message, responsive action is taken. Using routing information to determine whether a source of an infected message should be notified is disclosed. In some embodiments, if routing information for a prior message from the source of an infected message is similar to corresponding information for the infected message, the source is notified.

AMENDMENTS TO THE SPECIFICATION

Please replace paragraphs 0056-0057 with the following rewritten paragraphs:

[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 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~~ their web site. 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 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 no notification is made, or 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 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.

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 identifying a message as suspicious, comprising:

extracting from a received email message ~~an identity of~~ a sender of the received message; wherein the sender is an email address;

retrieving a prior routing data associated with a prior email message received previously from the sender; and

identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message.

2. (original) A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. (original) A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

4. (canceled)

5. (currently amended) A method as recited in claim 1, wherein identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message includes:

determining a first source IP address associated with the ~~prior~~ received message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

6. (currently amended) A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received email message ~~an identity of~~ a sender of the received message;

wherein the sender is an email address;

retrieve a prior routing data associated with a prior email message received previously from the sender; and

identify the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message; and

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

7. (original) A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. (original) A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

9. (canceled)

10. (currently amended) A system as recited in claim 6, wherein the processor is configured to identify the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message at least in part by:

determining a first source IP address associated with the ~~prior~~ received message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

11. (currently amended) A computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

extracting from a received email message ~~an identity of~~ a sender of the received message;

wherein the sender is an email address;

retrieving a prior routing data associated with a prior email message received previously from the sender; and

identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message.

12. (original) A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. (original) A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

14. (canceled)

15. (currently amended) A computer program product as recited in claim 11, wherein identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message includes:

determining a first source IP address associated with the ~~prior~~ received message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

16. (currently amended) A method for reporting a malicious network communication, comprising:

determining that a received network communication ~~comprises malicious data~~ is associated with an infection;

extracting first routing information from the received network communication;

~~retrieving corresponding prior~~ determining whether second routing information from a prior network communication received previously ~~from a sender with which the received network communication is associated; and~~ matches the first routing information;

~~notifying the sender~~ sending a notification that the received network communication ~~included malicious data~~ was associated with an infection ~~if a comparison of the routing information extracted from the received network communication to the prior routing information does not indicate~~ it is determined that the ~~received network communication~~ first routing

information and the ~~prior network communication came from different originating sources~~ second routing information match.

17. (canceled)

18. (new) The method of claim 16, wherein sending the notification includes sending the notification to a sender associated with the prior network communication.

19. (new) The method of claim 16, wherein sending the notification includes sending the notification to a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication.

20. (new) The method of claim 16, wherein the first routing information is associated with an IP address.

21. (new) The method of claim 16, wherein determining whether the first routing information and the second routing information match includes determining whether the first routing information and the second routing information are associated with the same geographical region.

22. (new) The method of claim 16, wherein the received network communication is associated with email.

23. (new) The method of claim 16, wherein the received network communication is associated with an instant message.

24. (new) The method of claim 16, wherein the prior network communication is associated with email.

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on March 5, 2009 between the Examiner and the undersigned Applicant. The Office Action mailed on October 6, 2008 was discussed. Specifically, the rejection of claim 11 under 35 USC 101, the rejection of claims 1, 6, and 11 under 35 USC 102 in light of Doyle et al (U.S. Patent Publication No. 2003/0043853), the rejection of claim 16 under 35 USC 103 in light of Mastrianni (US Patent Publication No. 2002/0116641 A1) and Tsuchiya et al (US 7,360,086 B1), and potential amendments to claims 1, 6, 11 and 16, were discussed with the intent to place the claims in better condition for allowance or appeal.

Applicant wishes to thank the Examiner for his time and attention in this case.

REMARKS

Claims 1-3, 5-8, 10-13, 15, 16, and 18-24 are pending. Claims 4, 9, 14, and 17 have been canceled. Claims 1, 5, 6, 10, 11, 15, and 16 have been amended. New claims 18-24 have been added. Support for the amendments and new claims can be found without limitation at paragraphs 56-58, and Figures 18, 19A, and 19B, of the specification.

The Examiner has objected to the Drawings on the basis that they do not show an "instant messaging session" or a "geographical region." Replacement sheets 23 and 24 (showing replacement Figures 18 and 19A respectively) are attached.

The Examiner has objected to the Abstract of the disclosure on the basis that the page containing the Abstract also contains the title. A replacement Abstract page has been provided.

The Examiner has objected to the Specification on the grounds that it contains an "embedded hyperlink and/or other form of browser-executable code" at paragraph 56. The Specification has been amended.

Applicant has discovered an omission in paragraph 57 of the Specification, and correspondingly at 1906 of Figure 19A. The Specification and Figure have been amended. Support for the modification may be found at page 34, line 15 of provisional application 60/613,909, to which the Application claims priority.

The Examiner has rejected claims 11-15 under 35 USC 101 as being directed to non-statutory subject matter. Claim 11 has been amended and is believed to be allowable. Claim 14 has been canceled Claims 12, 13, and 15 depend from claim 11 and are believed to be allowable for the reasons described above.

The Examiner has rejected claims 5, 10, and 15 under 35 USC 112 as being indefinite. Claims 5, 10, and 15 have been amended and are believed to be allowable.

The Examiner has rejected claims 1-3, 6-8, and 11-13 under 35 USC 102(b) as being anticipated by Doyle et al (US 2003/0043853 A1), hereinafter referred to as Doyle. Doyle purports to teach "methods, systems and computer program products ...for determining if a packet has a spoofed source Internet Protocol (IP) address." (Doyle, Abstract.)

Doyle does not appear to teach or suggest "extracting from a received email message a sender of the received message; wherein the sender is an email address," nor "retrieving a prior routing data associated with a prior email message received previously from the sender," as recited in amended independent claims 1 and 11, and similarly in amended independent claim 6.

Claims 1, 6, and 11 are therefore believed to be allowable.

Claims 2 and 3 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claims 7 and 8 depend from claim 6 and are believed to be allowable for the same reasons described above.

Claims 12 and 13 depend from claim 11 and are believed to be allowable for the same reasons described above.

The Examiner has rejected claims 4, 9, and 14 under 35 USC 103(a) as being unpatentable over Doyle in view of Banister et al (US 2004/0260778 A1). Claims 4, 9, and 14 have been canceled without prejudice.

The Examiner has rejected claims 5, 10, and 15 under 35 USC 103(a) as being unpatentable over Doyle in view of Sobel et al (US 7366919 B1), hereinafter referred to as Sobel. Sobel purports to teach "Computer implemented methods, apparati, and computer-readable media for detecting suspected spam in email...originating from a sending computer... A method embodiment comprises the steps of determining...the actual IP address...of the sending computer...; converting...the actual IP address...into geo-location data; and, using the geo-location data, ascertaining...whether the e-mail...contains suspected spam." (Sobel, Abstract.)

Neither Doyle nor Sobel, alone or in combination, appear to teach or suggest "extracting from a received email message a sender of the received message; wherein the sender is an email address; retrieving a prior routing data associated with a prior email message received previously from the sender," as recited in amended independent claims 1 and 11, and similarly in amended independent claim 6.

Claims 1, 6, and 11 are therefore believed to be allowable.

Claim 5 depends from claim 1 and is believed to be allowable for the same reasons described above.

Claim 10 depends from claim 6 and is believed to be allowable for the same reasons described above.

Claim 15 depends from claim 11 and is believed to be allowable for the same reasons described above.

The Examiner has rejected claims 16 and 17 under 35 USC 103(a) as being unpatentable over Mastrianni (US 2002/0116641 A1) in view of Tsuchiya et al (US 7360086 B1), hereinafter referred to as Tsuchiya.

Neither Mastrianni nor Tsuchiya, alone or in combination, appear to teach or suggest "determining that a received network communication is associated with an infection" nor "sending a notification that the received network communication was associated with an infection it is determined that the first routing information and the second routing information match," as recited in amended independent claim 16.

Claim 16 is therefore believed to be allowable. Claim 17 has been canceled. New claims 18-24 depend from claim 16 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: March 5, 2009

Inventor

Aaron Emigh
Customer #85853
762 Judith Court
Incline Village, NV 89451
Tel. 415-297-1305

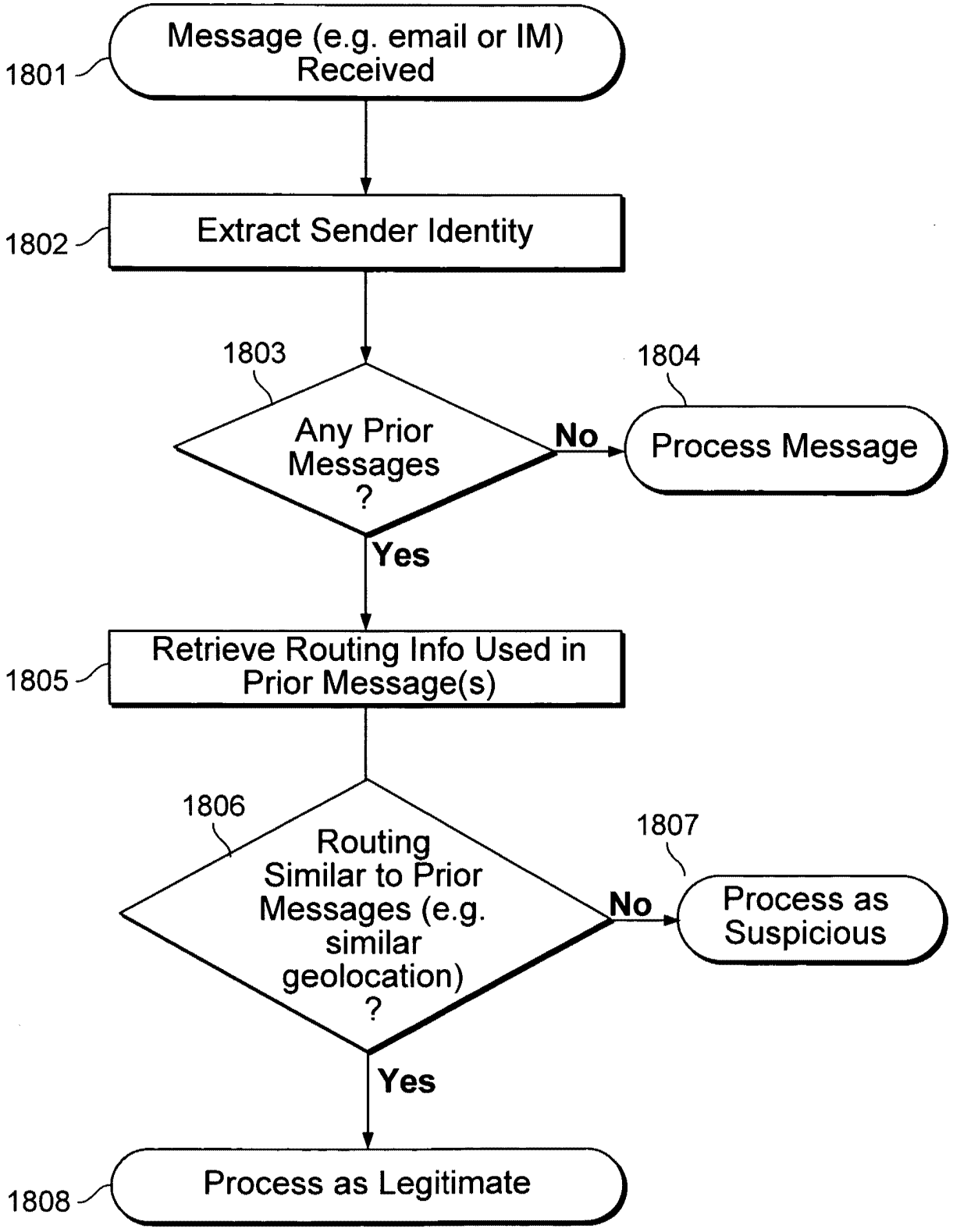

1801
Message (e.g. email or IM) Received
1802
Extract Sender Identity
1803
Any Prior Messages ?
No
1804
Process Message
Yes
1805
Retrieve Routing Info Used in Prior Message(s)
1806
Routing Similar to Prior Messages (e.g. similar geolocation) ?
No
1807
Process as Suspicious
Yes
1808
Process as Legitimate

FIG. 18

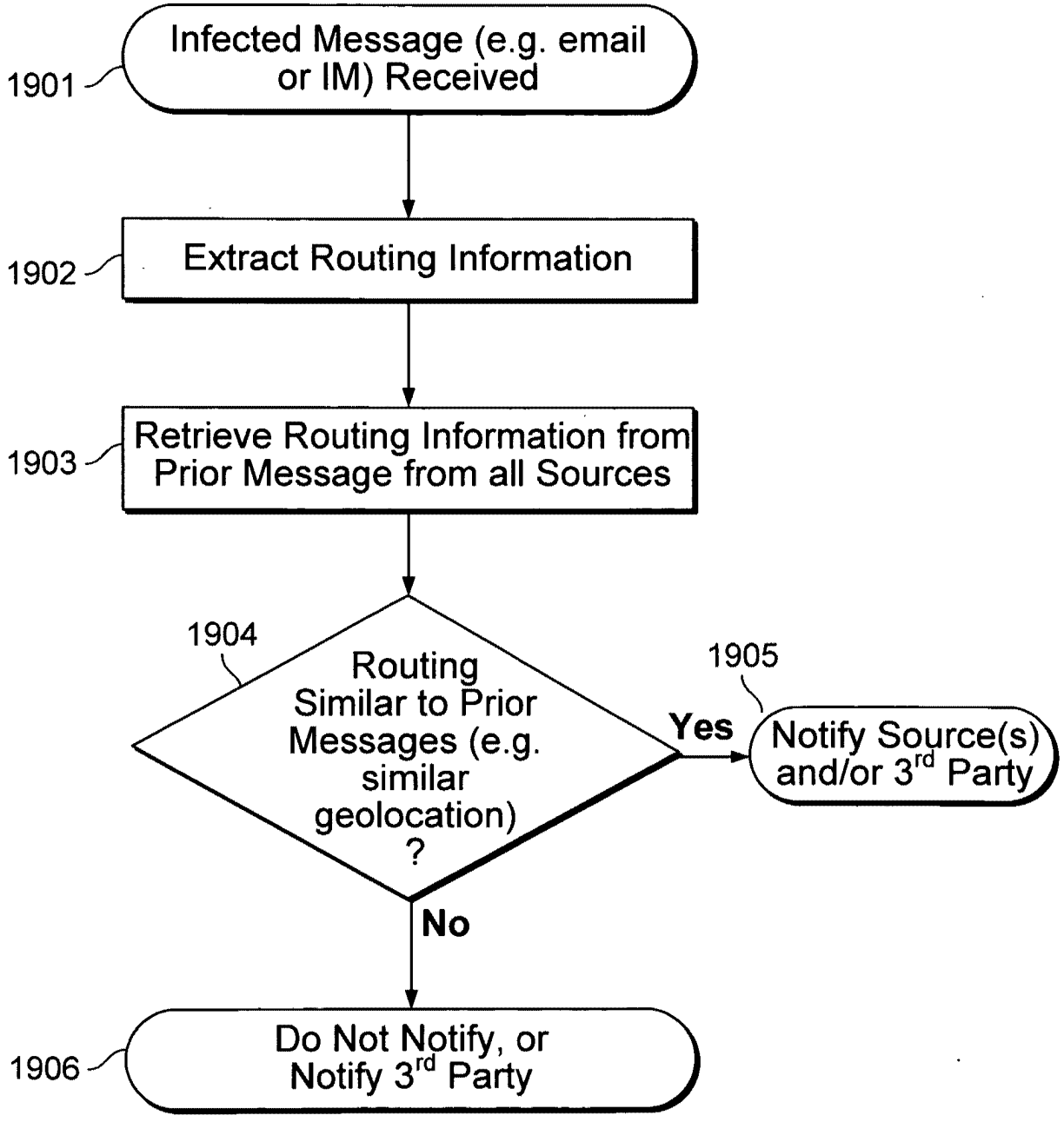

1901
Infected Message (e.g. email or IM) Received
1902
Extract Routing Information
1903
Retrieve Routing Information from Prior Message from all Sources
1904
Routing Similar to Prior Messages (e.g. similar geolocation) ?
Yes
1905
Notify Source(s) and/or 3rd Party
No
1906
Do Not Notify, or Notify 3rd Party

FIG. 19A

OIPE
MAR 09 2009
PATENT & TRADEMARK OFFICE
IAP78

DFW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.:	PB-036
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

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

March 5, 2009. _____
Inventor

TRANSMITTAL OF AMENDMENT A

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

Sir:

Transmitted herewith is Amendment A in response to Office Action mailed October 6, 2008 in the above-identified application.

Applicant(s) hereby petition for the following extension of time in which to respond to the outstanding Office Action.

		SMALL ENTITY	
		Rate	Add'l Fee
☐ Extension for Response within FIRST month		x $65 = $	
☒ Extension for Response within SECOND month	1	x $245 = $	245
☐ Extension for Response within THIRD month		x $555 = $	
☐ Extension for Response within FOURTH month		x $865 = $	
☐ Extension for Response within FIFTH month		x $1175 = $	

03/09/2009 NNGUYEN1 00000039 11237004
01 FC:2252 245.00 OP

Enclosed is Radix Holdings, LLC Check No. 1012 in the amount of $245.00 to cover the additional extension of time fees.

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-036).

Respectfully submitted,



Aaron Emigh
Inventor

Customer #85853
Aaron Emigh
762 Judith Court
Incline Village, NV 89451
Tel. 415-297-1305

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
11/237,004	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	03/09/2009	(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))	* 20	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 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 ($)	ADDITIONAL FEE ($)	OR	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 LANFORD/

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/237,004	09/27/2005	James A. Roskind	PB-036

CONFIRMATION NO. 6024

POWER OF ATTORNEY NOTICE

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

OC000000034808822

Date Mailed: 03/06/2009

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

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
11/237,004	09/27/2005	James A. Roskind	RAD2P003

CONFIRMATION NO. 6024

85853
Aaron Emigh
762 Judith Court
Incline Village, NV 89451

POA ACCEPTANCE LETTER

OC000000034808859

Date Mailed: 03/06/2009

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

OIPE
FEB 23 2009
PATENT & TRADEMARK OFFICE

JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Weidner, Timothy J.
Application No.:	11/237,004	Art Unit:	2419
Filed:	9/27/2005	Docket No.	RAD2P003

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

JTN

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	11/237,004
Filing Date	9/27/2005
First Named Inventor	Roskind
Art Unit	2419
Examiner Name	Weidner, Timothy J.
Attorney Docket Number	RAD2P003

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).

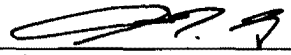
I am the:

☑ 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	Telephone
January 26, 2009	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	11/237,004
Filing Date	9/27/2005
First Named Inventor	Roskind
Art Unit	2419
Examiner Name	Weidner, Timothy J.
Attorney Docket Number	RAD2P003

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.

OIPE
FEB 23 2009
USPTO
PATENT & TRADEMARK OFFICE

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

COVER LETTER

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

Sir:

Transmitted herewith are:

1. Change of Correspondence Address forms PTO/SB/122 changing Correspondence Addresses to customer #85853 for applications 11/237,004, 11/237,199, 11/237,003, 11/131,038, 11/069,288, 11/061,498, 11/061,488, 11/054,799, 11/054,800, 11/016,150, 11/011,879, 11/011,870, 11/011,214, 11/011,874, 11/011,873, 11/995,748, 10/984,435, 10/982,714, 10/982,971, 10/983,126, 10/967,552, 10/967,553, 10/915,213, 10/915,240, 10/914,794, and 10/914,908 (two forms for each application); and

2. Revocation of Power of Attorney for applications 11/237,003, 11/237,199, and 11/237,004.

The Commissioner is hereby authorized to charge any fees required to Deposit Account No. 50-4831 (Applicant Docket No. COA).

Respectfully submitted,

Aaron Emigh
Inventor

Aaron Emigh
Customer #85853
762 Judith Court
Incline Village, NV 89451
Tel. 415-297-1305

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
11/237,004	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 01/11/2009

	(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))	* 20	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 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:
/DEBORAH NASH/

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.
11/237,004	09/27/2005	James A. Roskind	RAD2P003	6024

21912 7590 10/06/2008

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
WEIDNER, TIMOTHY J	

ART UNIT	PAPER NUMBER
2419	

MAIL DATE	DELIVERY MODE
10/06/2008	PAPER

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

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/237,004	ROSKIND ET AL.	
	Examiner	Art Unit	
	Timothy J. Weidner	2619	

-- 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) *1-17* 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) *1-17* 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 *21 February 2006* 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

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the instant messaging session (claims 4, 9, and 14) and the geographical region (claims 5, 10, and 15) must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

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

Specification

The abstract of the disclosure is objected to because the title is on the same page as the abstract. Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code (paragraph 56). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 101

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

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

Claims 11-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims are directed to "computer program product" which is software per se (paragraph 42, line 25). Further, “computer readable medium” is tied to program instructions sent over a communications link (paragraph 29, lines 1-4). Software and signals do not fall into one of the four statutory categories of invention, i.e. process, machine, manufacture, or composition of matter.

Claim Rejections - 35 USC § 112

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.

Claims 5, 10, and 15 are 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.

Regarding claims 5, 10, and 15, lines 5-6, 6-7, and 6-7 respectively, it is unclear how the first and second source addresses are both associated with the prior message. It appears one of the source addresses should be associated with a current message.

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 –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 6-8, and 11-13 are rejected under 35 U.S.C. 102(b) as being anticipated by Doyle et al. (US 2003/0043853 A1).

Regarding claims 1, 6, and 11, Doyle teaches extracting from a received message a MAC address (identity) of a sender of the received message (paragraph 69, lines 1-7), retrieving an IP address (prior routing data) (paragraph 71, lines 12-14) associated with a prior message received previously from the sender (paragraphs 69, lines 5-6), and discarding the packet (identifying the received message as suspicious) if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicated the received message was received

from a different originating source than the prior message (paragraph 71, lines 17-20; different source IP addresses).

Further, regarding apparatus and computer readable medium claims 6 and 11, Doyle teaches a processor and memory together performs the steps of the method (paragraph 32-33).

Regarding claims 2, 7, and 12, Doyle teaches processing the received message normally if it is determined that no prior routing data associated with the sender is available (paragraph 69, lines 1-3 and 11-13).

Regarding claims 3, 8, and 13, Doyle teaches the prior routing data includes data extracted from a header portion of the prior message (paragraph 52, lines 4-6).

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.

Claims 4, 9, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) as applied to claims 1, 6, and 11 above, in view of Banister et al. (US 2004/0260778 A1).

Regarding claims 4, 9, and 14, Doyle teaches the prior routing data includes an IP address (paragraph 71, lines 12-14), but may not explicitly teach an instant messaging session.

Banister, which is in the same field of endeavor, teaches network address verification using instant messages for the purpose of fining users for sending spam (paragraphs 50 and 56). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the prior routing data include an IP address retrieved from a prior instant messaging session to fine users for sending spam.

Claims 5, 10, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2003/0043853 A1) as applied to claims 1, 6, and 11 above, in view of Sobel et al. (US 7366919 B1).

Regarding claims 5, 10, and 15, Doyle teaches determining a first source IP address associated with the prior message (paragraph 71, lines 12-14), and determining a second source IP address associated with the message (paragraph 69, lines 1-7). However, Doyle may not explicitly teach determining whether the first and second IP addresses are associated with the same geographical region.

Sobel, which is in the same field of endeavor, teaches resolving two IP addresses into geographical regions and determining whether they are the same for the purpose of detecting spam (column 5, lines 15-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine whether the first and second source addresses belong to the same geographical region to detect spam.

Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mastrianni (US 2002/0116641 A1) in view of Tsuchiya et al. (US 7360086 B1).

Regarding claim 16, Mastrianni teaches determining that a received network communication comprises an objectionable source (malicious data) (paragraph 44), extracting the IP address (routing information) from the received network communication (paragraph 44), and retrieving prior routing information from a prior network communication received previously from a sender with which the received network communication is associated (paragraph 44). Mastrianni may not explicitly teach notifying the sender that the received network communication included malicious data if a comparison of the routing information extracted from the received network communication to the prior routing information does not indicate they came from different originating sources.

Tsuchiya, which is in the same field of endeavor, teaches notifying the sender when a comparison of two IP addresses reveals a coincidence in address (column 9, lines 40-52) for the purpose of notifying the sender of a successful move between ports (column 9, lines 3-8). It would have been obvious to one of ordinary skill in the art at the time the invention was made to notify the sender that current and prior routing information does not indicate they came from different originating sources to notify the sender of a successful move between ports.

Regarding claim 17, Mastrianni may not explicitly teach notifying a third party in the even of a comparison of prior and current routing information indicating they came from different originating sources.

Tsuchiya teaches notifying a true user (3rd party) and not the sender when a comparison of two IP addresses reveals no coincidence (columns 11-12, lines 56-7) for

the purpose of rapid recovery of failure due to an erroneously set IP address (column 11, liens 1-9). It would have been obvious to one of ordinary skill in the art at the time the invention was made to notify a third party, and not the sender, that current and prior routing information indicates they came from different originating sources to rapidly recover a failure due to an erroneously set IP address.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Timothy J. Weidner whose telephone number is (571) 270-1825. The examiner can normally be reached on Monday - Friday, 8:00 AM - 5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. 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.

/Timothy J Weidner/
Examiner, Art Unit 2619

/Wing F. Chan/
Supervisory Patent Examiner,
Art Unit 2619
9/30/08

Notice of References Cited	Application/Control No. 11/237,004	Applicant(s)/Patent Under Reexamination ROSKIND ET AL.	
	Examiner Timothy J. Weidner	Art Unit 2619	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0043853 A1	03-2003	Doyle et al.	370/489
*	B	US-7,366,919 b1	04-2008	Sobel et al.	726/23
*	C	US-2004/0260778 a1	12-2004	Banister et al.	709/206
*	D	US-2002/0116641 a1	08-2002	Mastrianni, Steven J.	713/201
*	E	US-7,360,086 b1	04-2008	Tsuchiya et al.	713/168
*	F	US-2003/0035370 a1	02-2003	Brustoloni, Jose?apos, C.	370/229
*	G	US-2004/0181694 a1	09-2004	Cox et al.	713/201
*	H	US-2004/0078485 a1	04-2004	Narayanan, Ram Gopal Lakshmi	709/242
*	I	US-2004/0205135 a1	10-2004	Hallam-Baker, Phillip Martin	709/206
*	J	US-2005/0198159 a1	09-2005	Kirsch, Steven T.	709/206
*	K	US-2006/0028996 a1	02-2006	Huegen et al.	370/252
	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
	11237004	ROSKIND ET AL.
	Examiner	**Art Unit**
	Timothy J Weidner	2619

✓	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	09/29/2008								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11237004	ROSKIND ET AL.
	Examiner	Art Unit
	Timothy J Weidner	2619

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
eDAN inventorship search	9/25/2008	TJW
EAST search class/sub 370/252,389,401 713/153,154 726/22,26,27 using keywords	9/29/2008	TJW

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	22	("20020010800" | "20030014665" | "20030126468" | "20040078485" | "20040146006" | "20050213570" | "20050074001" | "20060029104" | "6851028" | "7299296" | "7328451"). PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 14:29
S2	4682	370/252.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:14
S3	2429	S2 and address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:15
S4	861	S2 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:15
S5	208	S2 and IP adj address with (compar$4 differen$5 match $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:16
S6	3634	S2 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:21
S7	161	S6 and S5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:21

S8	68	S7 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 15:22
S9	668	sender near id and (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:17
S10	263	sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:18
S11	0	S2 and S10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:18
S12	251	713/154.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:18
S13	1	S9 and S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:18
S14	986	713/153.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:19
S15	7	S9 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:19

S16	0	S9 and IP near spoof$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:22
S17	129	S12 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:24
S18	66	S17 and source near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:24
S19	64	S18 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 16:24
S20	206	S9 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 17:02
S21	90	S10 and IP adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 17:02
S22	48	S21 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 17:02
S24	0	S5 and S9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 17:35

S25	2	"20070014276".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 17:55
S26	2	"20030035370".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/25 18:06
S27	25	"726".clas. and sender near id same (email e adj mail)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 08:43
S28	211	(sender near id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 08:50
S29	144	S28 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 08:51
S30	11	"370".clas. and S29	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 08:51
S31	19	"713".clas. and S29 not S30	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 08:56
S32	8	"726".clas. and S29 not (S30 S31)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 09:05

S33	106	S29 not (S30 S31 S32)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 09:11
S34	3	(mailfrom mail adj from) and (email e adj mail instant near message) and (IP adj address) not S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 10:51
S35	1297	726/22.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 15:10
S37	249	S35 and (email e adj mail instant near messag$3) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 15:11
S38	52	S35 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 15:11
S39	44	S38 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/26 15:12
S42	1770	726/26.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:13
S43	1174	726/27.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:13

S44	5668	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:14
S45	20	S42 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:17
S46	19	S45 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:17
S47	5	S43 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:17
S48	5	S47 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:17
S49	125	S44 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:18
S50	0	S44 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:18
S51	1	S44 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:19

S52	7499	370/401.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:19
S53	1	S52 and (mailfrom mail adj from senderid sender adj id) and (email e adj mail instant near message) and (IP adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:19
S54	178	S52 and (email e adj mail instant near messag$3) and (IP adj address) and (source adj address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:20
S55	143	S54 and (@ad<"20040927" @prad<"20040927" @rlad<"20040927")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:20
S56	177	S52 and (email e adj mail instant near messag$3) same ((IP adj address) (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:20
S57	8	S52 and (email e adj mail instant near messag$3) same ((IP adj address) and (source adj address))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/29 09:20

9/30/2008 8:55:33 AM
C:\Documents and Settings\tweidner\My Documents\EAST\Workspaces\11237004.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. 6024

SERIAL NUMBER	FILING or 371(c) DATE / RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/237,004	09/27/2005	379	2619	RAD2P003

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 **
12/22/2005

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☐ No	/TIMOTHY J WEIDNER/ Examiner's Signature	☐ Initials	CA	25	17	4

ADDRESS

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014
UNITED STATES

TITLE

Detecting and processing suspicious network communications

FILING FEE RECEIVED		
600	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

OIPE
FEB 21 2006
PATENT & TRADEMARK OFFICE
IAP67

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	ROSKIND et al.	Examiner:	Not Assigned
Application No.:	11/237,004	Art Unit:	2645
Filed:	September 27, 2005	Docket No.:	RAD2P003
Title:	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS		

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:

Feb. 18 2006.

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 December 23, 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: Twenty-Five (25) Sheets of Replacement Drawings

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 $	0		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. RAD2P003).

☒ 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. RAD2P003).

☒ 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: 2/16/06

William J. James
Reg. No. 40,661

OIPE IAP67
FEB 21 2006
PATENT & TRADEMARK OFFICE

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
11/237,004	09/27/2005	James A. Roskind	RAD2P003

CONFIRMATION NO. 6024

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FORMALITIES LETTER

Date Mailed: 12/23/2005

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- 3d, 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 MUST be returned with the reply.

H. Ahmed

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

OIPE
FEB 21 2006
IAP67
PATENT & TRADEMARK OFFICE

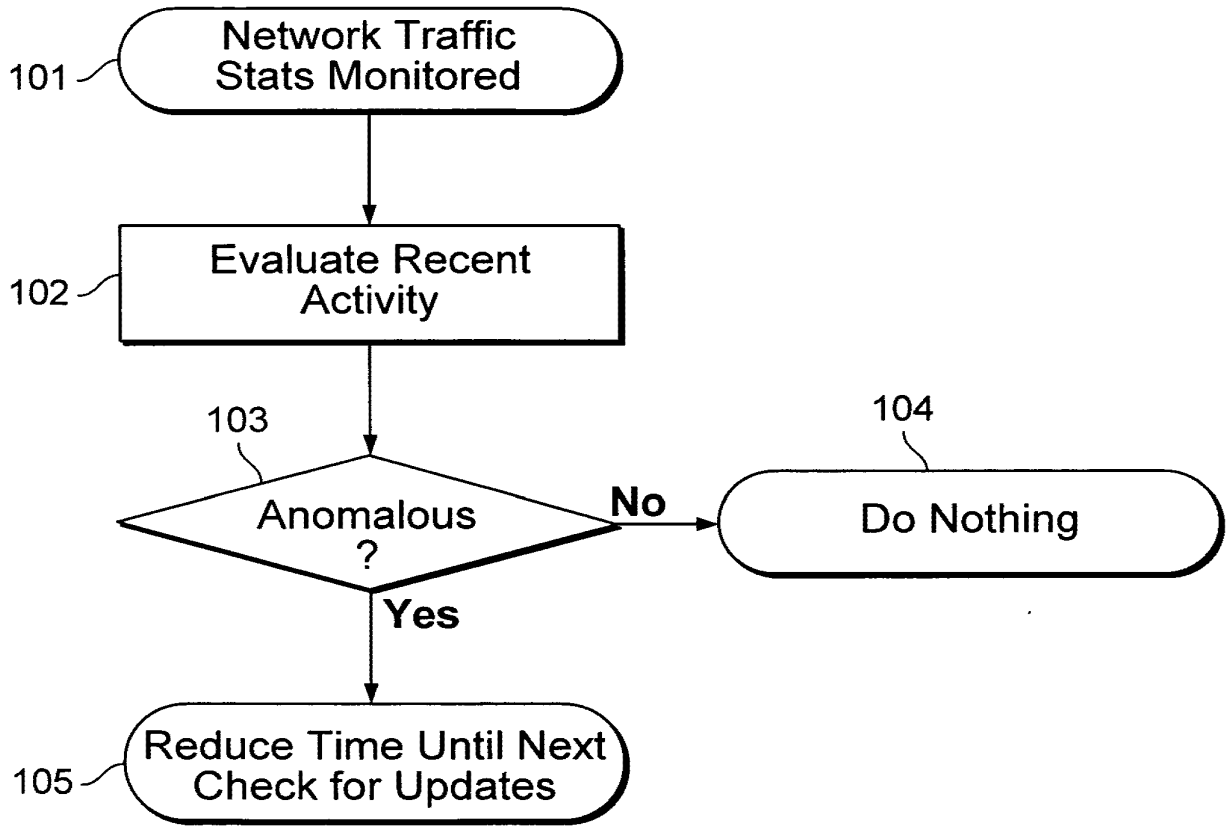


FIG. 1

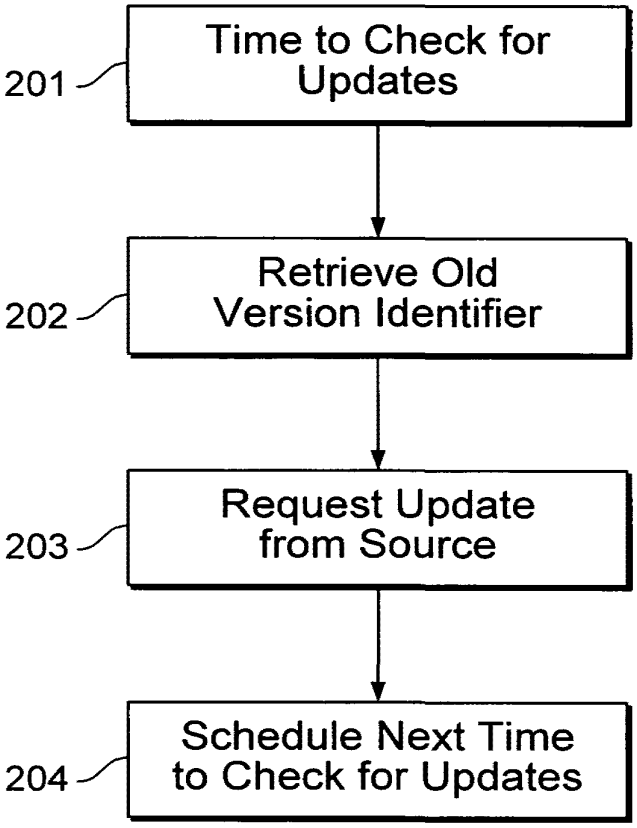

201
Time to Check for Updates
202
Retrieve Old Version Identifier
203
Request Update from Source
204
Schedule Next Time to Check for Updates

FIG. 2A

3/25

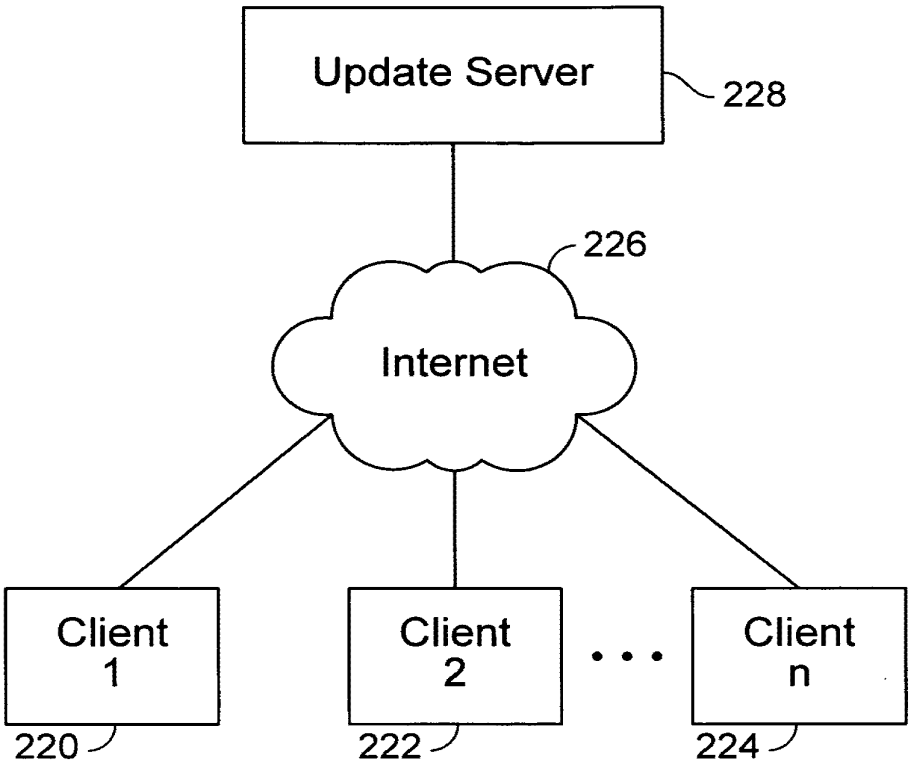

Update Server
228
226
Internet
Client 1
Client 2
Client n
220
222
224

FIG. 2B

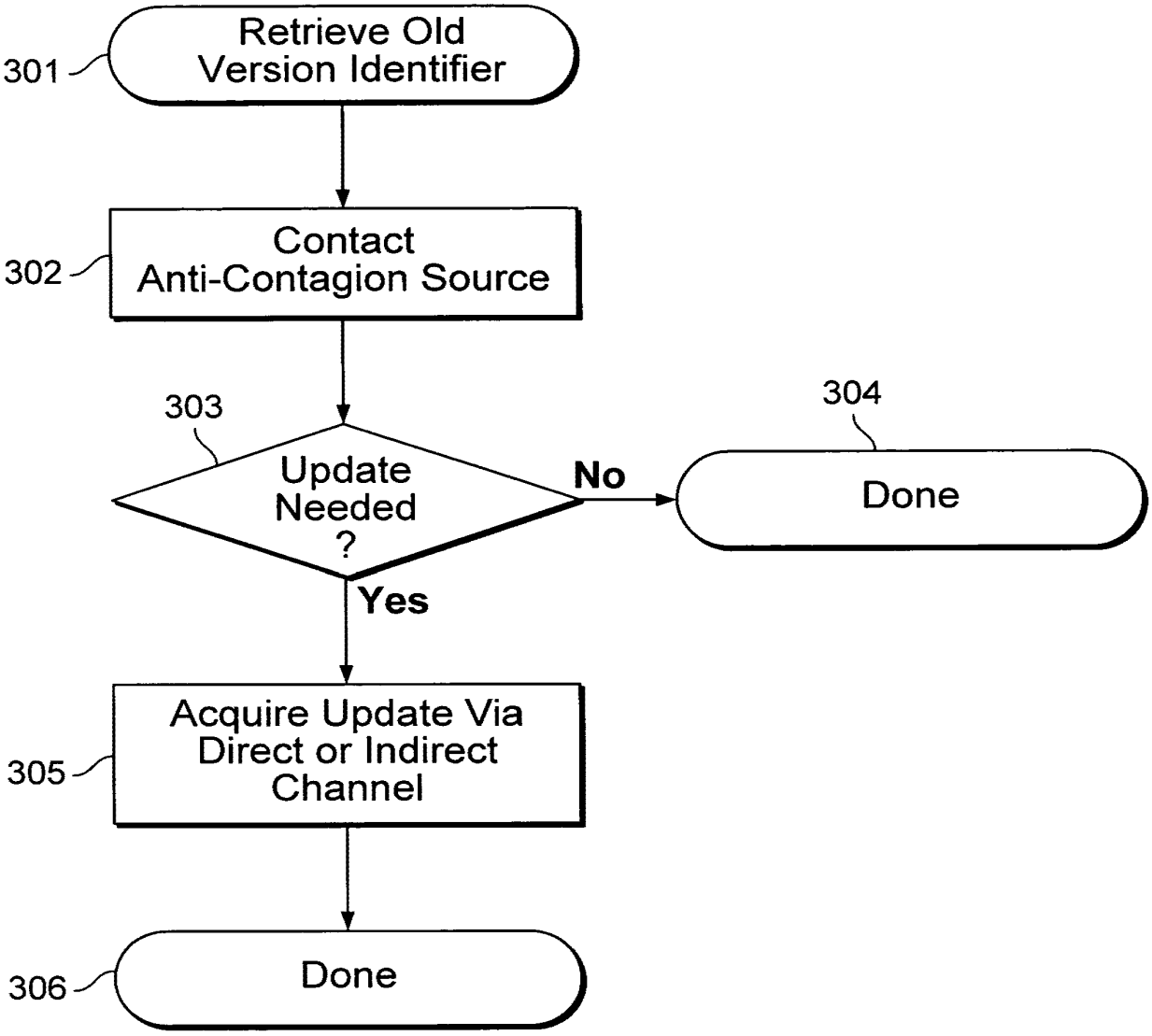

301
Retrieve Old Version Identifier
302
Contact Anti-Contagion Source
303
Update Needed ?
No
304
Done
Yes
305
Acquire Update Via Direct or Indirect Channel
306
Done

FIG. 3A

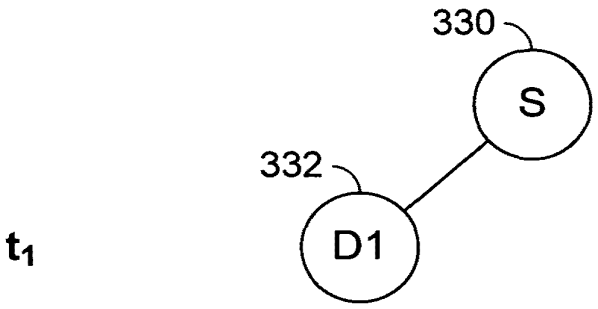


FIG. 3B

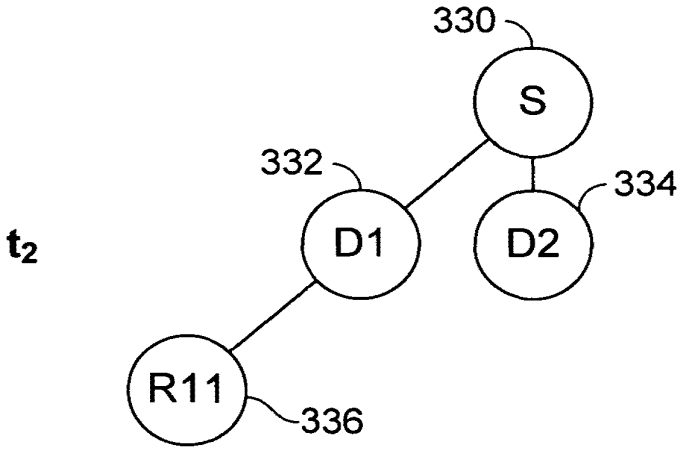


FIG. 3C

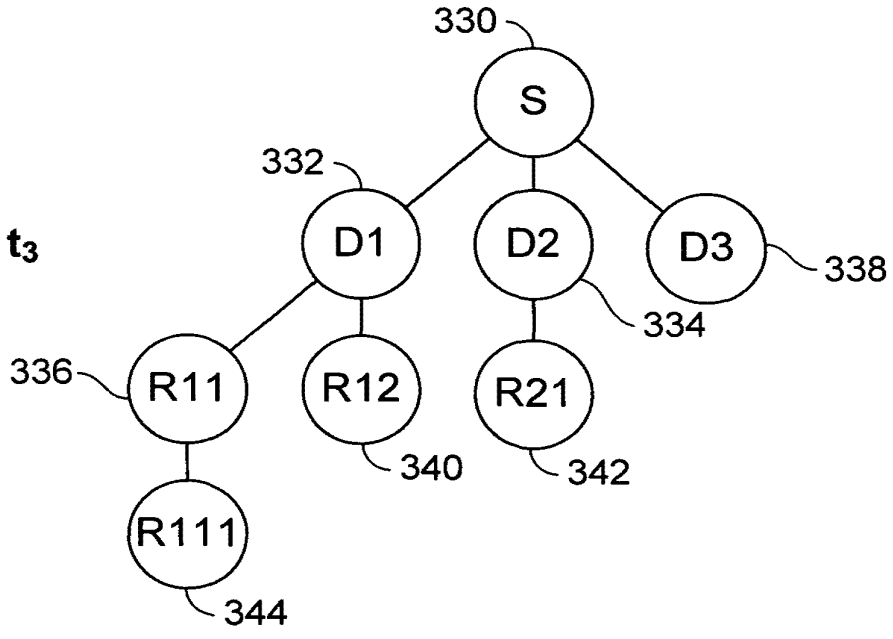


FIG. 3D

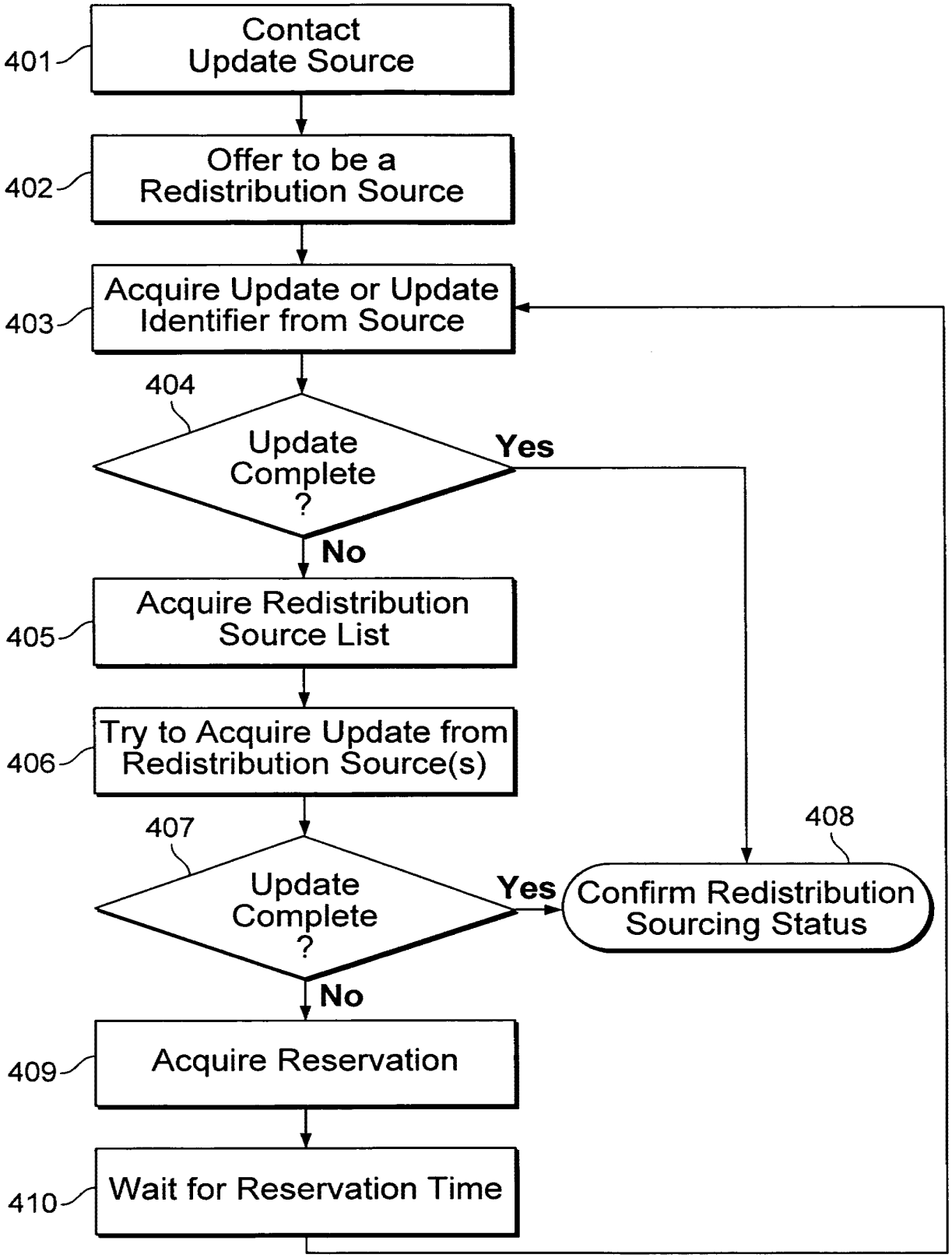

401
Contact Update Source
402
Offer to be a Redistribution Source
403
Acquire Update or Update Identifier from Source
404
Update Complete ?
Yes
No
405
Acquire Redistribution Source List
406
Try to Acquire Update from Redistribution Source(s)
407
Update Complete ?
Yes
No
408
Confirm Redistribution Sourcing Status
409
Acquire Reservation
410
Wait for Reservation Time

FIG. 4A

7/25

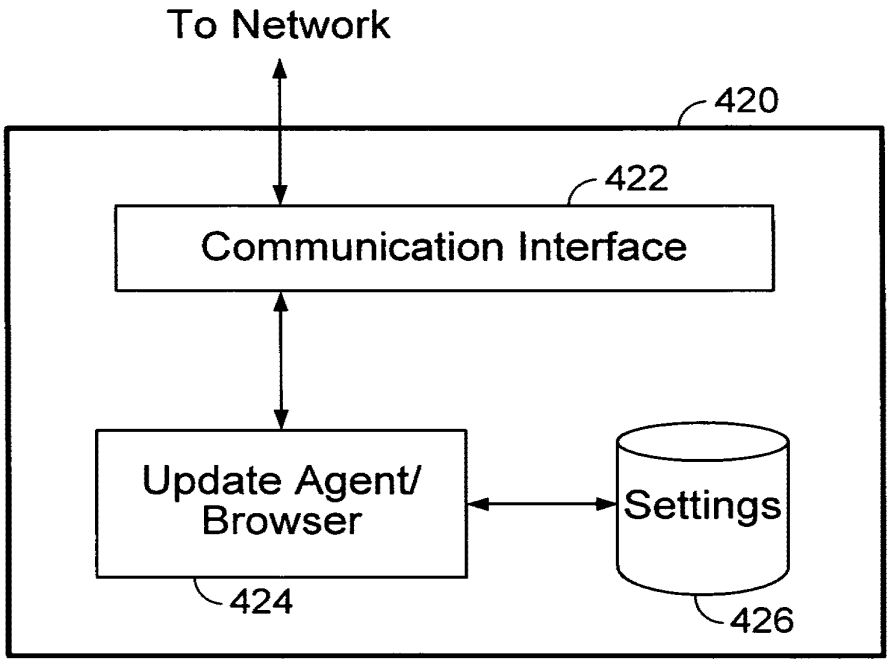

To Network
420
422
Communication Interface
Update Agent/
Browser
Settings
424
426

FIG. 4B

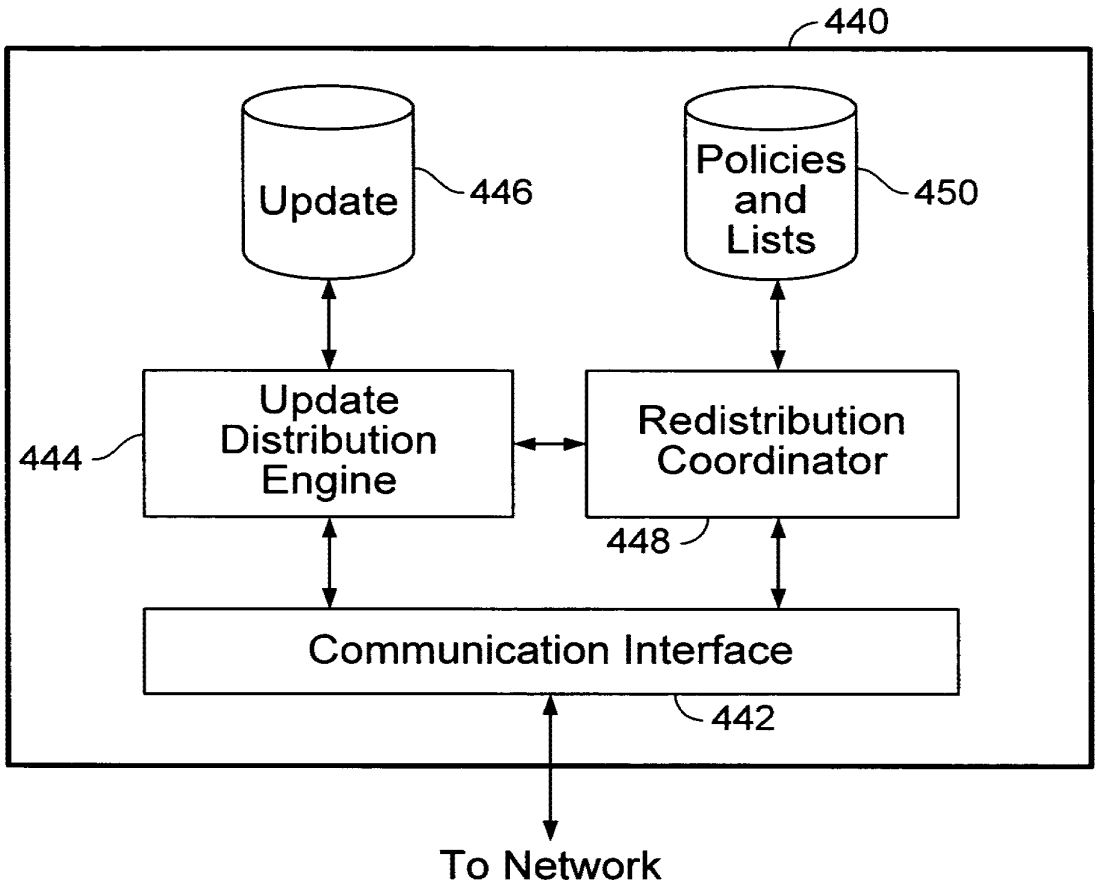

440
Update
446
Policies and Lists
450
Update Distribution Engine
444
Redistribution Coordinator
448
Communication Interface
442
To Network

FIG. 4C

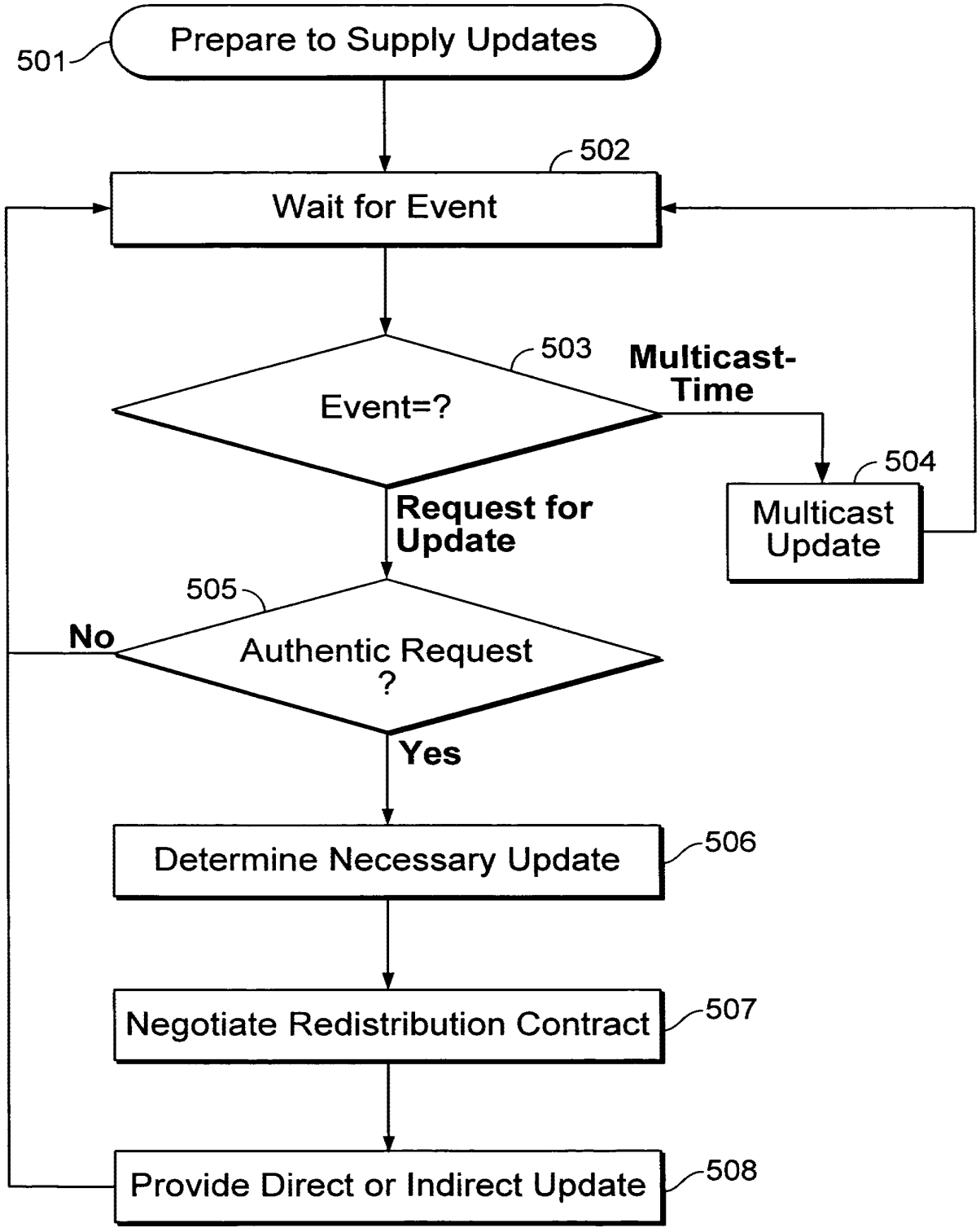

Prepare to Supply Updates
501
Wait for Event
502
Event=?
503
Multicast-Time
Request for Update
Multicast Update
504
Authentic Request ?
505
No
Yes
Determine Necessary Update
506
Negotiate Redistribution Contract
507
Provide Direct or Indirect Update
508

FIG. 5

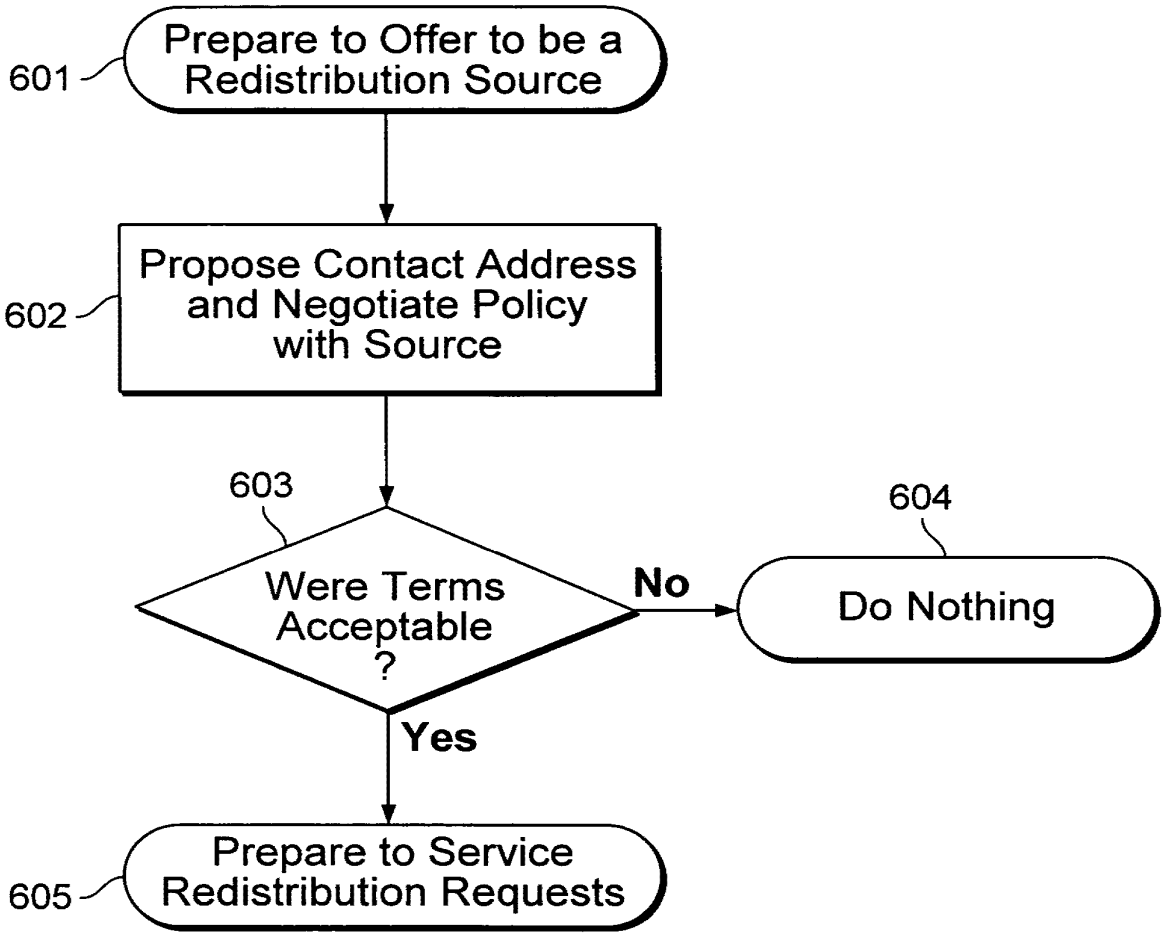

601
Prepare to Offer to be a Redistribution Source
602
Propose Contact Address and Negotiate Policy with Source
603
Were Terms Acceptable ?
No
604
Do Nothing
Yes
605
Prepare to Service Redistribution Requests

FIG. 6

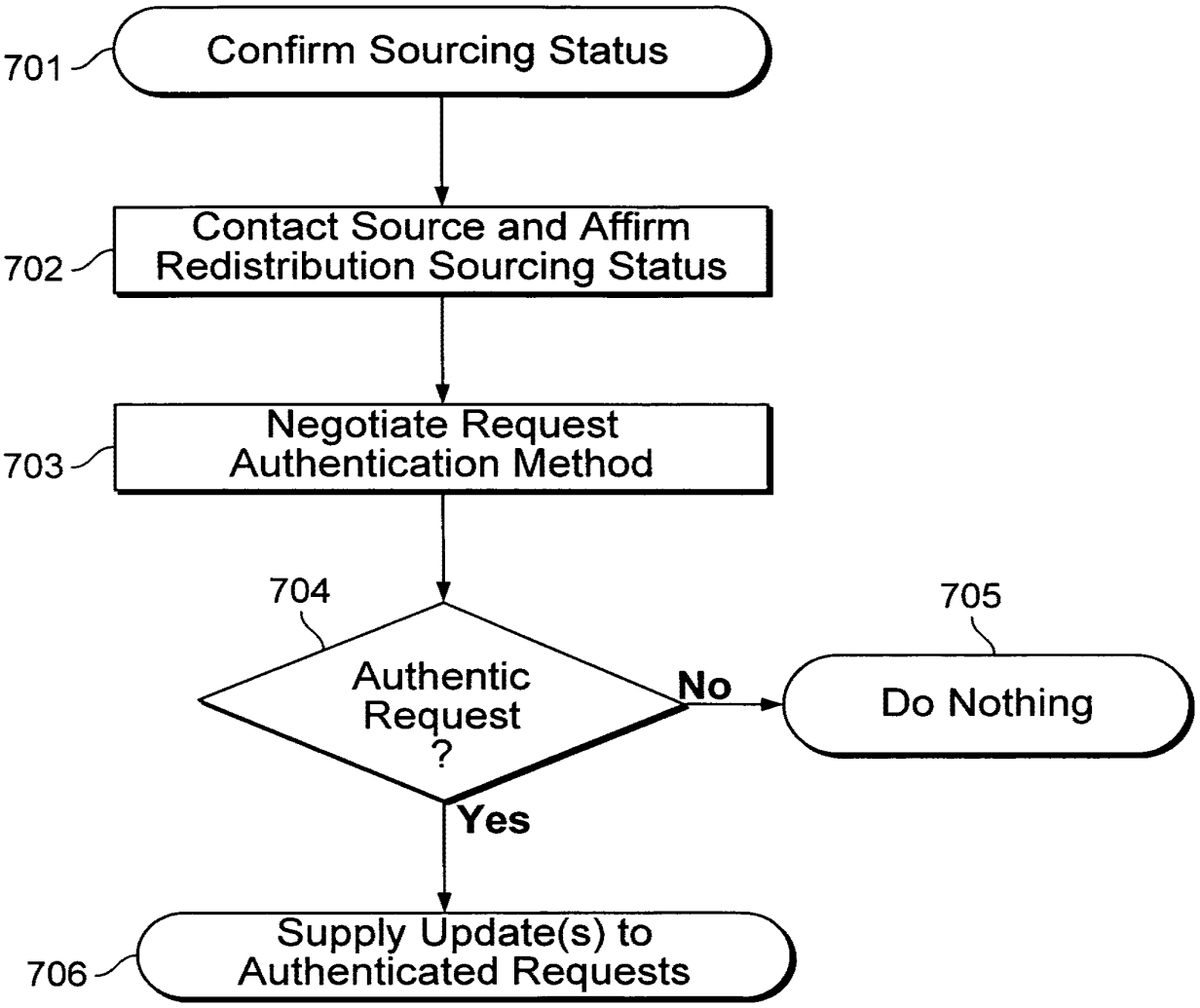

701
Confirm Sourcing Status
702
Contact Source and Affirm Redistribution Sourcing Status
703
Negotiate Request Authentication Method
704
Authentic Request ?
No
705
Do Nothing
Yes
706
Supply Update(s) to Authenticated Requests

FIG. 7

12/25

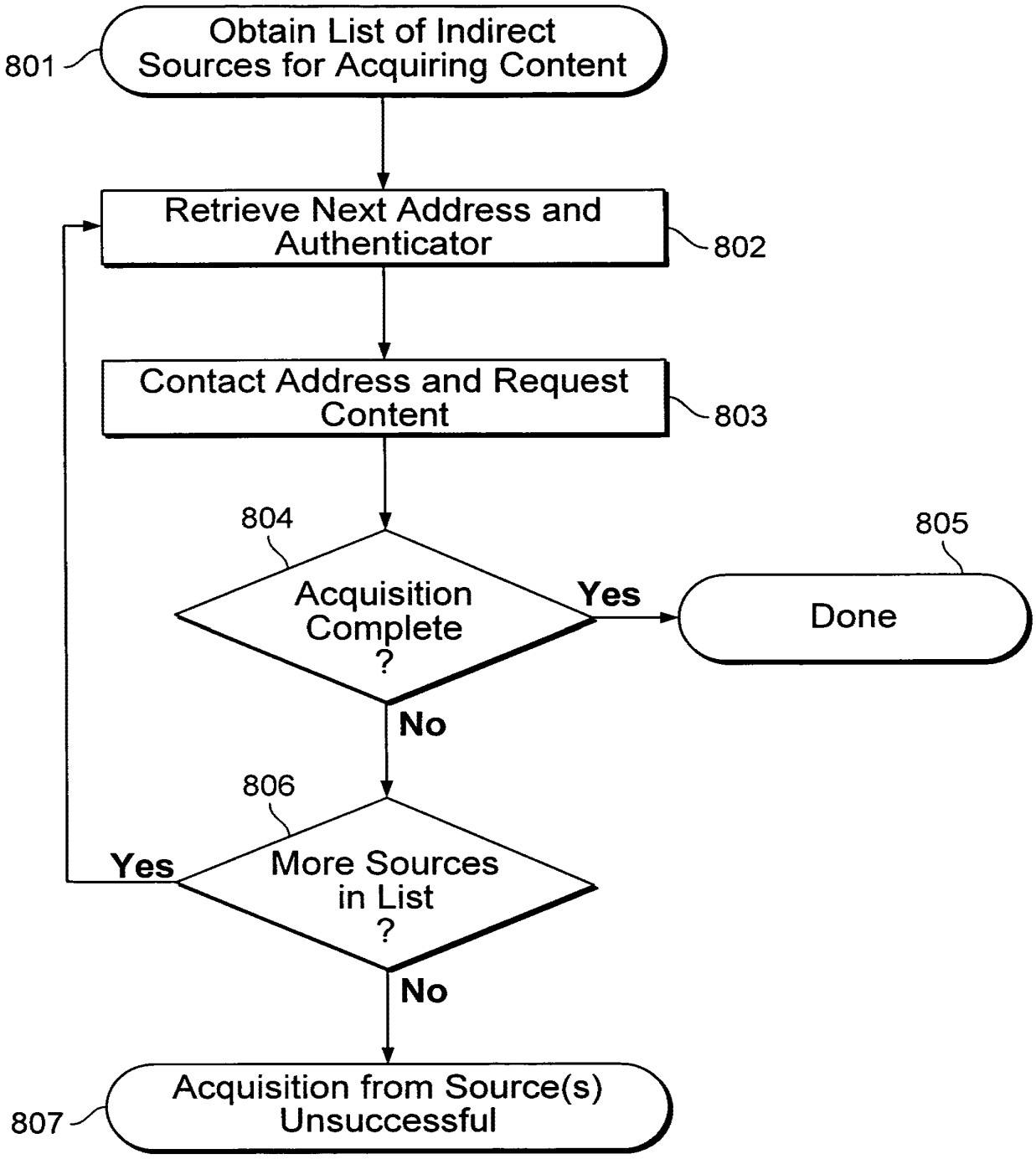

Obtain List of Indirect Sources for Acquiring Content
801
Retrieve Next Address and Authenticator
802
Contact Address and Request Content
803
804
Acquisition Complete ?
Yes
805
Done
No
806
More Sources in List ?
Yes
No
Acquisition from Source(s) Unsuccessful
807

FIG. 8

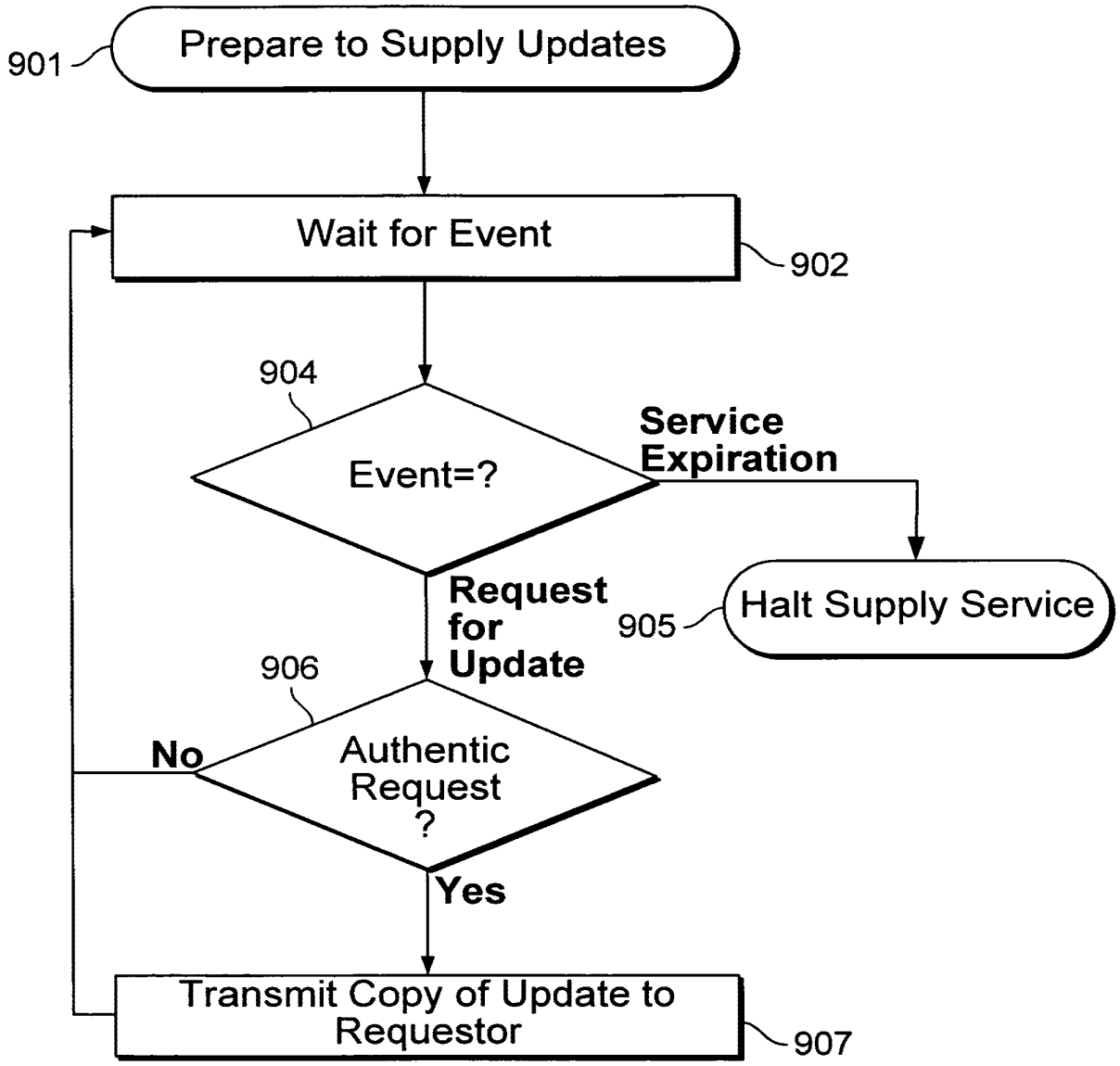

901
Prepare to Supply Updates
Wait for Event
902
904
Event=?
Service Expiration
905
Halt Supply Service
Request for Update
906
Authentic Request ?
No
Yes
Transmit Copy of Update to Requestor
907

FIG. 9

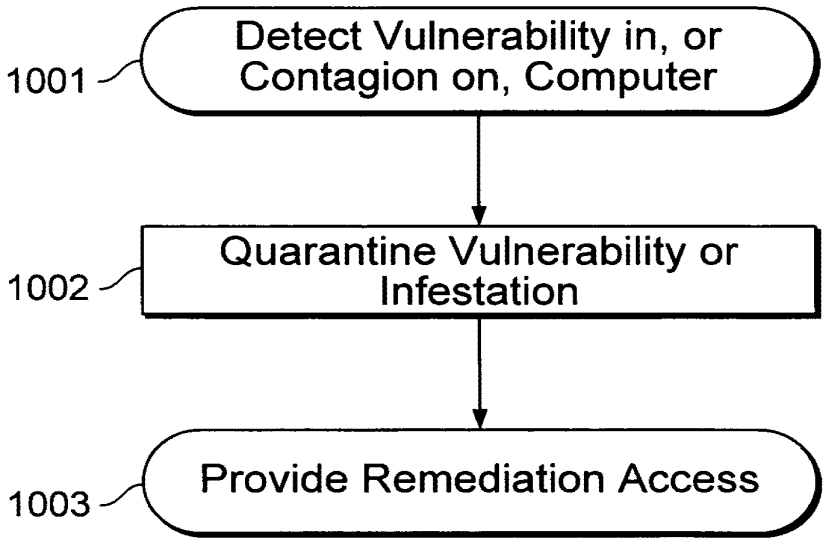

1001
Detect Vulnerability in, or Contagion on, Computer
1002
Quarantine Vulnerability or Infestation
1003
Provide Remediation Access

FIG. 10A

15/25

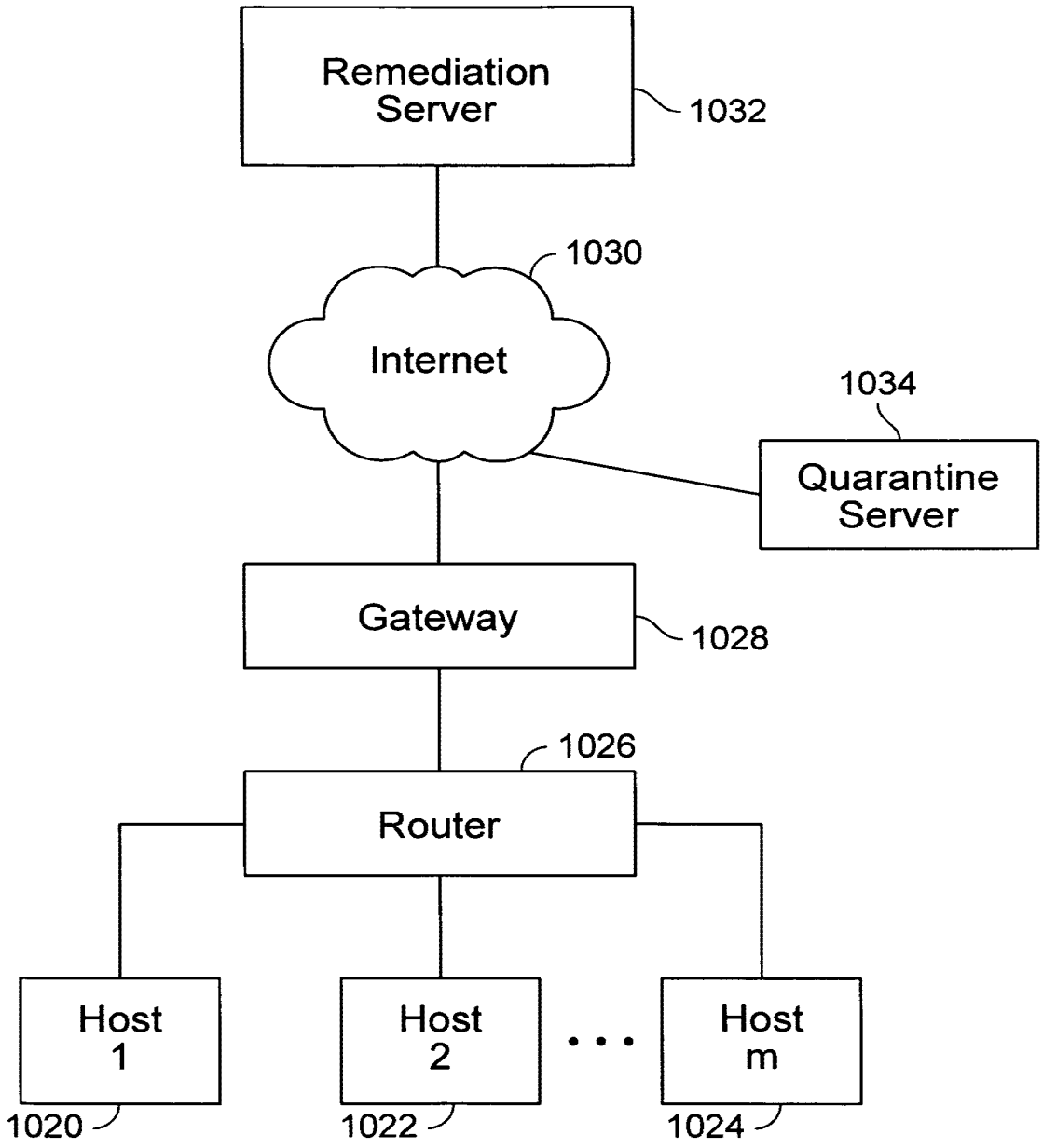

Remediation Server
1032
1030
Internet
1034
Quarantine Server
Gateway
1028
1026
Router
Host 1
Host 2
Host m
1020
1022
1024

FIG. 10B

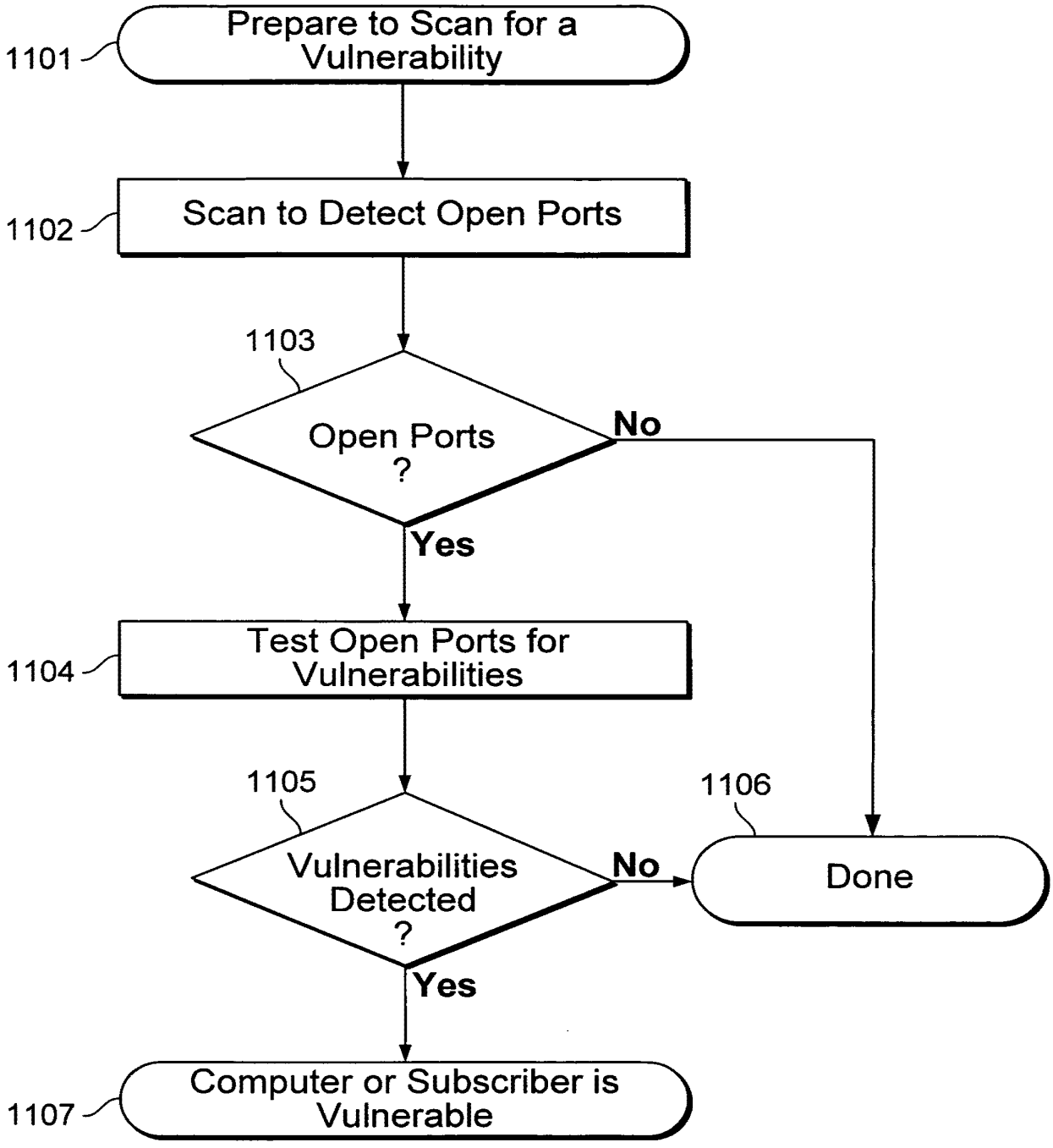

Prepare to Scan for a Vulnerability
1101
Scan to Detect Open Ports
1102
1103
Open Ports ?
No
Yes
Test Open Ports for Vulnerabilities
1104
1105
Vulnerabilities Detected ?
No
1106
Done
Yes
Computer or Subscriber is Vulnerable
1107

FIG. 11

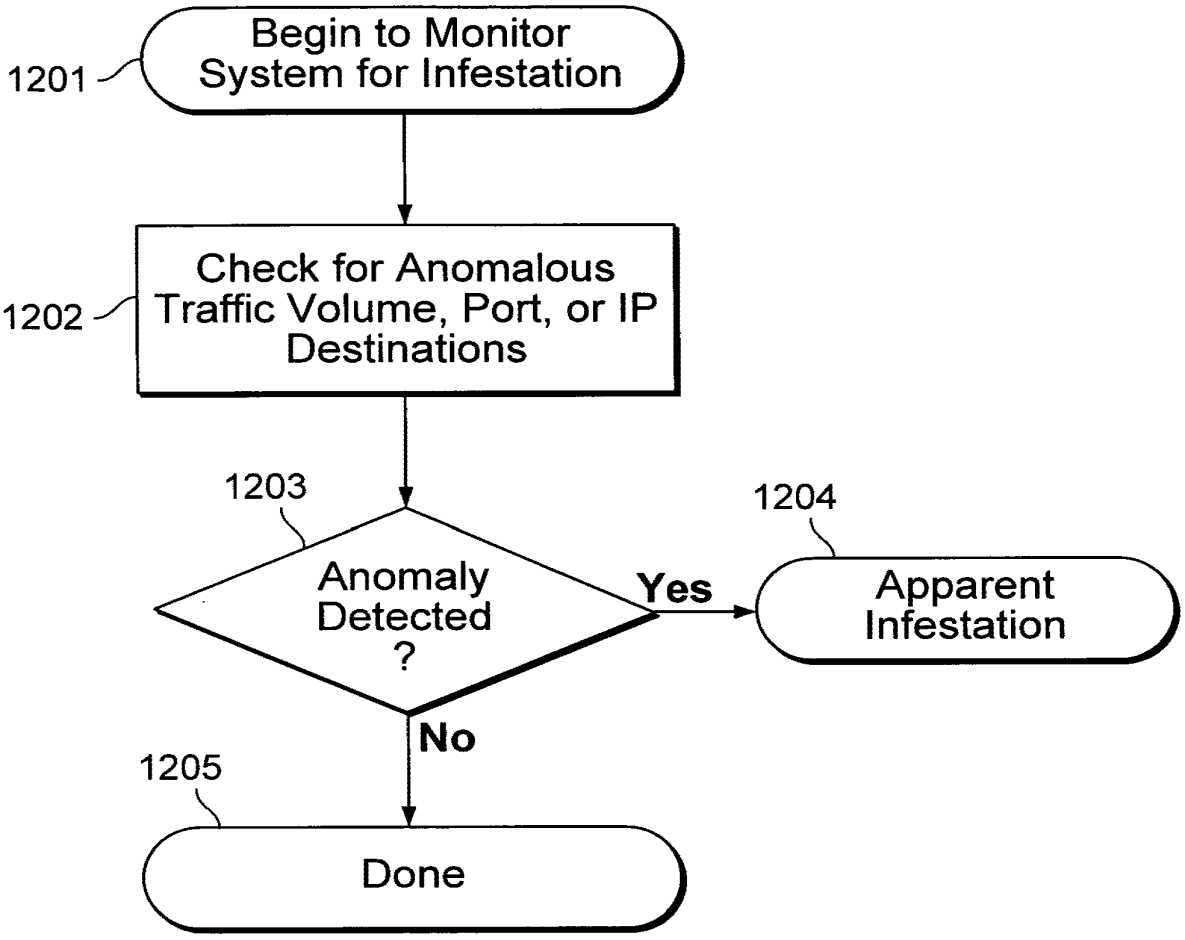

1201
Begin to Monitor System for Infestation
1202
Check for Anomalous Traffic Volume, Port, or IP Destinations
1203
Anomaly Detected ?
Yes
1204
Apparent Infestation
No
1205
Done

FIG. 12

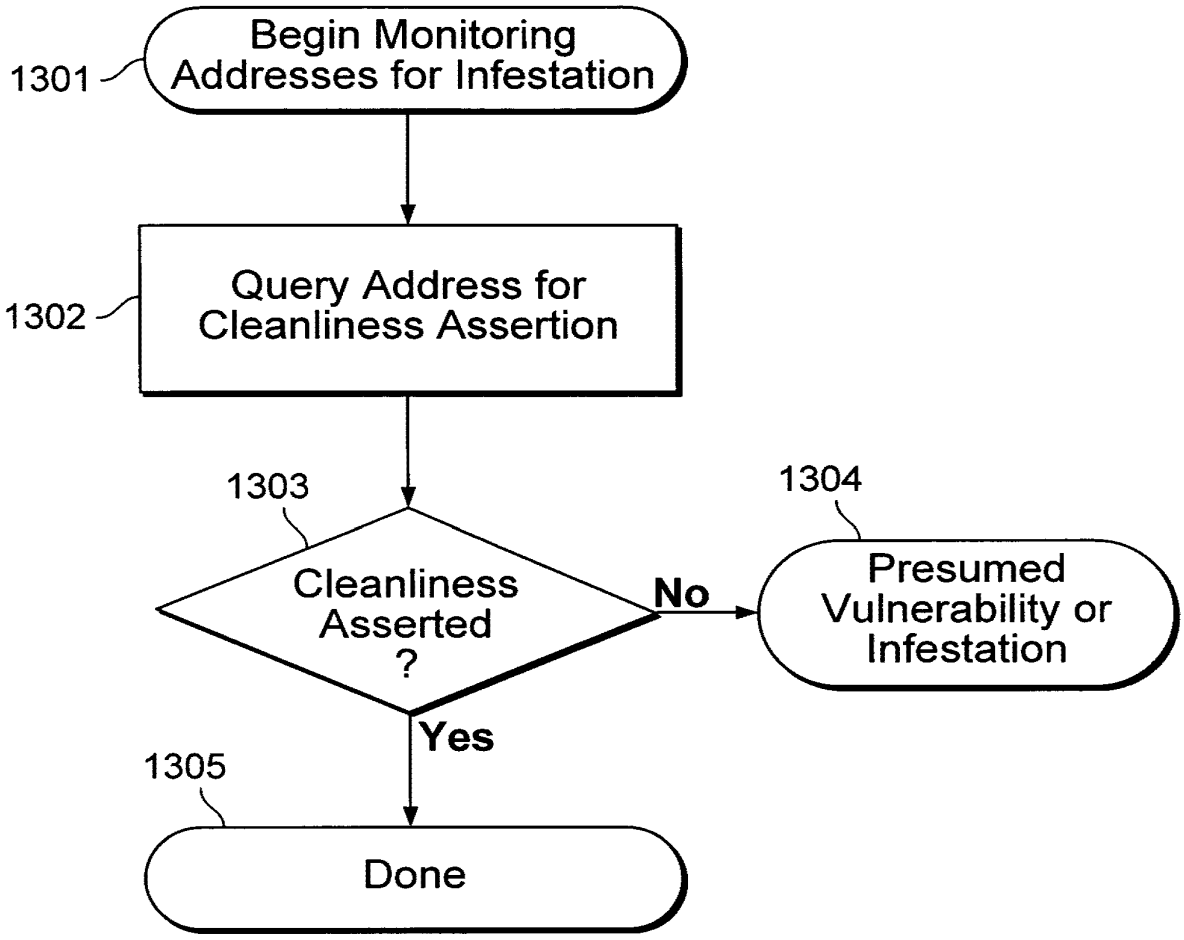

1301
Begin Monitoring Addresses for Infestation
1302
Query Address for Cleanliness Assertion
1303
Cleanliness Asserted ?
No
1304
Presumed Vulnerability or Infestation
Yes
1305
Done

FIG. 13

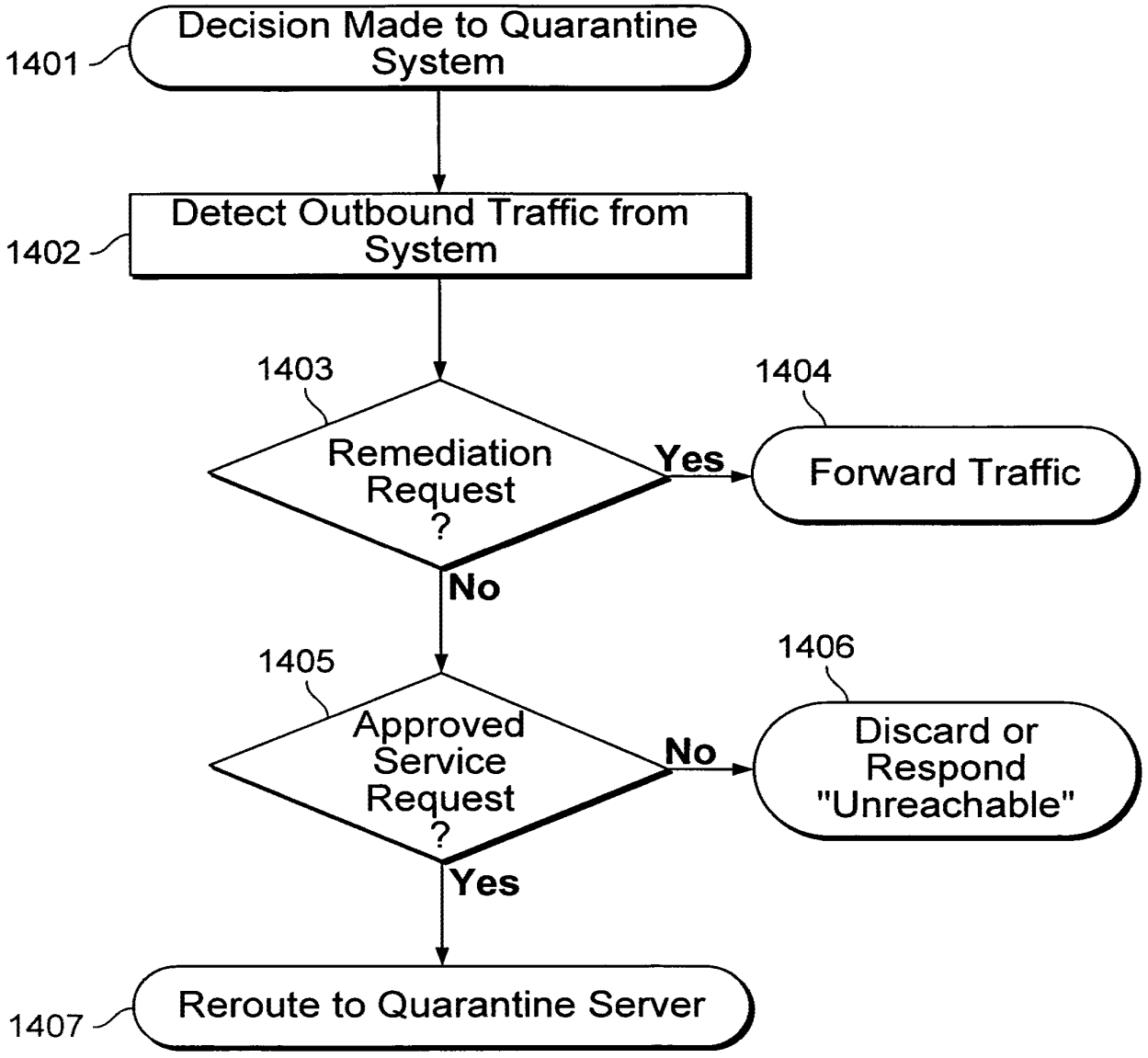

1401
Decision Made to Quarantine System
1402
Detect Outbound Traffic from System
1403
Remediation Request ?
Yes
1404
Forward Traffic
No
1405
Approved Service Request ?
No
1406
Discard or Respond "Unreachable"
Yes
1407
Reroute to Quarantine Server

FIG. 14

20/25

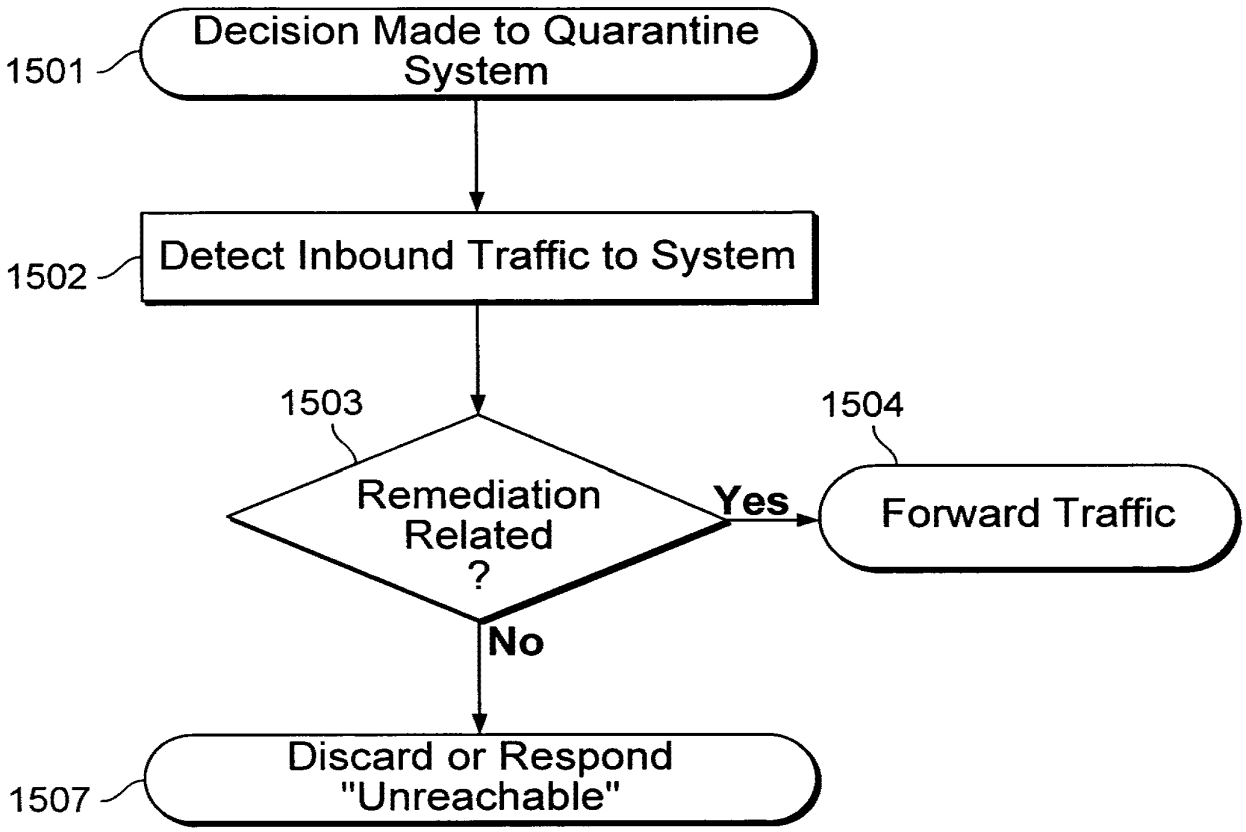

1501
Decision Made to Quarantine System
1502
Detect Inbound Traffic to System
1503
Remediation Related ?
Yes
1504
Forward Traffic
No
1507
Discard or Respond "Unreachable"

FIG. 15

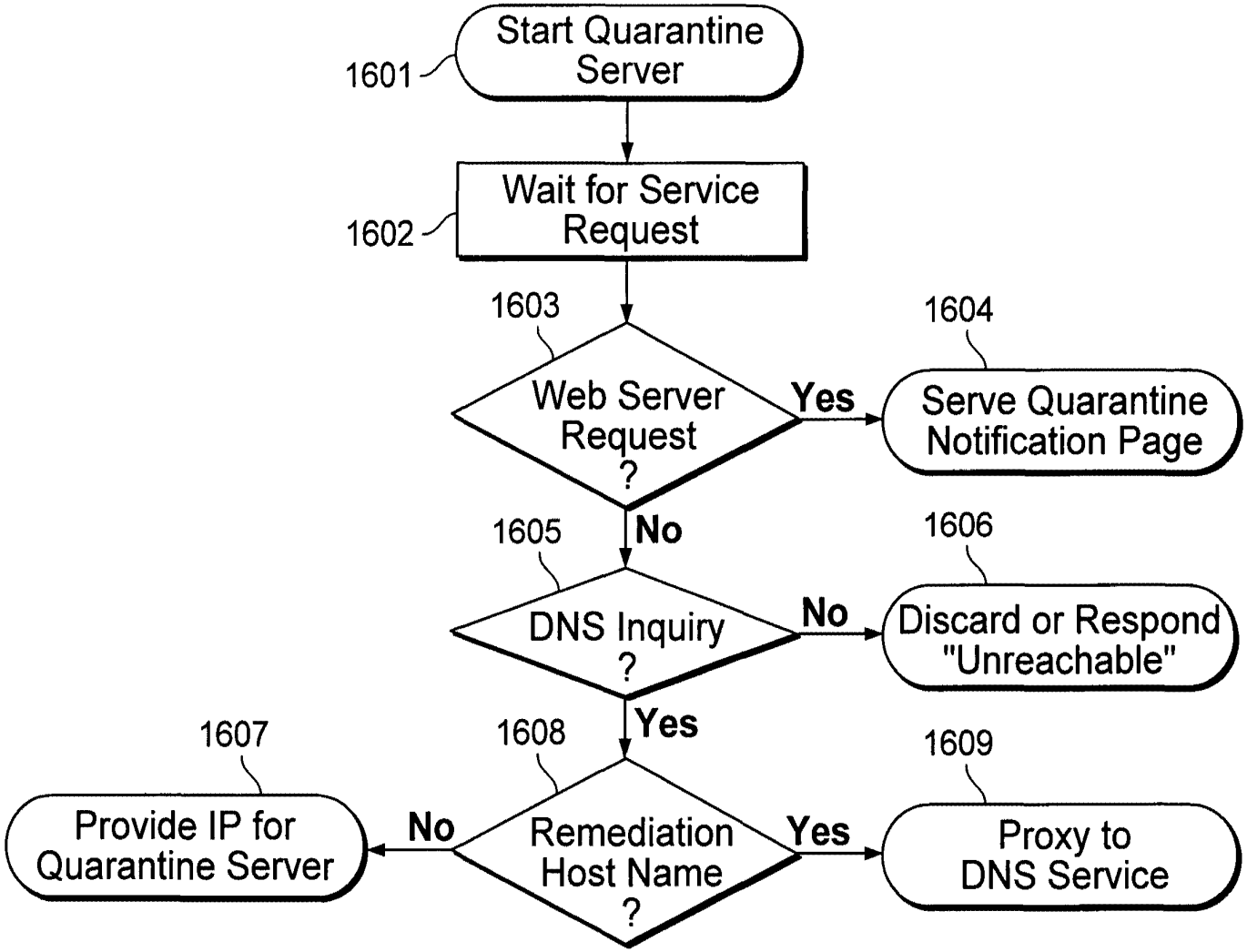


FIG. 16

REPLACEMENT SHEET
App. No.: 11/237,004
Att. Dkt. No.: RAD2P003
Sheet 21 of 25

22/25

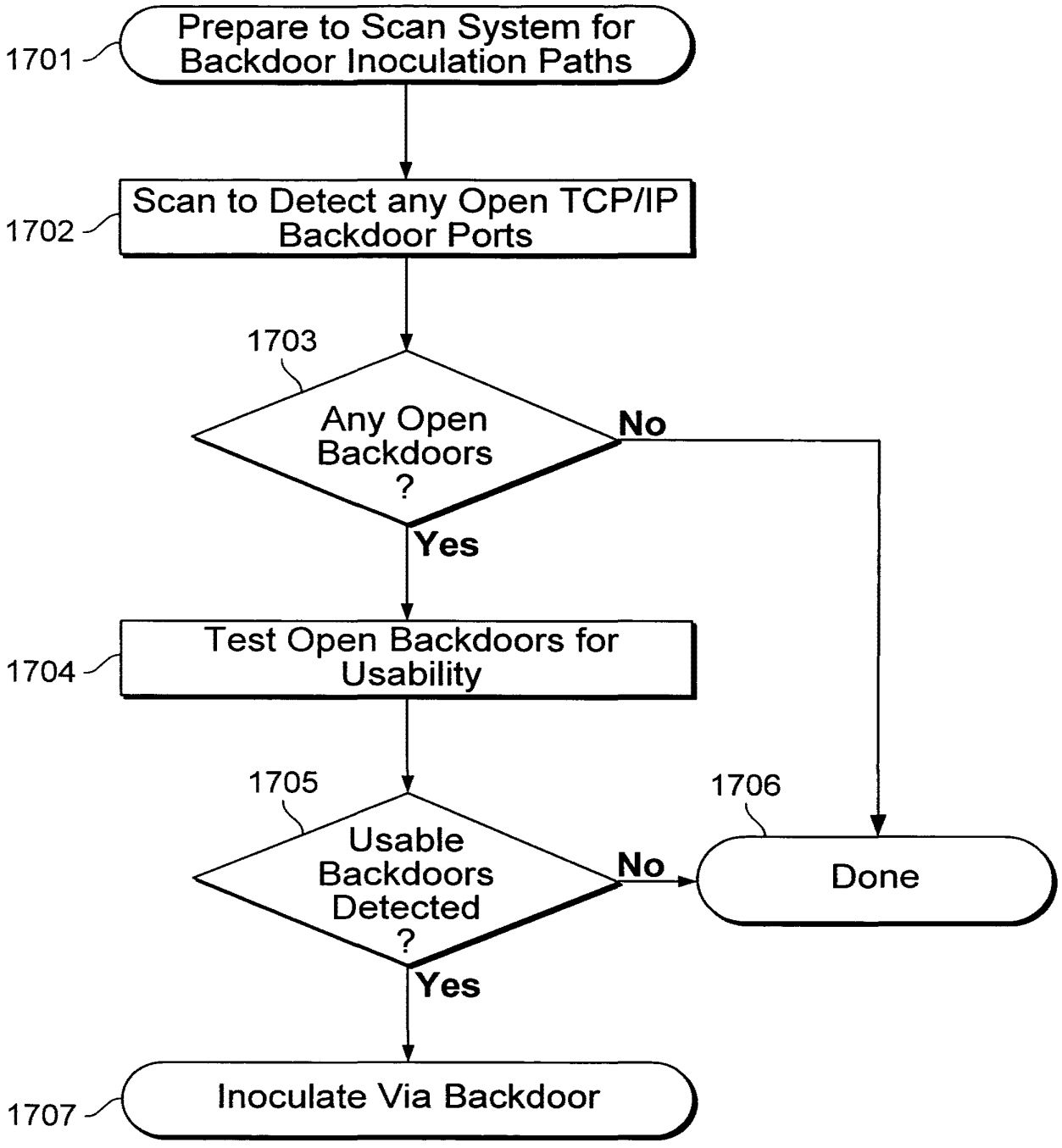

1701
Prepare to Scan System for Backdoor Inoculation Paths
1702
Scan to Detect any Open TCP/IP Backdoor Ports
1703
Any Open Backdoors ?
No
Yes
1704
Test Open Backdoors for Usability
1705
Usable Backdoors Detected ?
No
1706
Done
Yes
1707
Inoculate Via Backdoor

FIG. 17

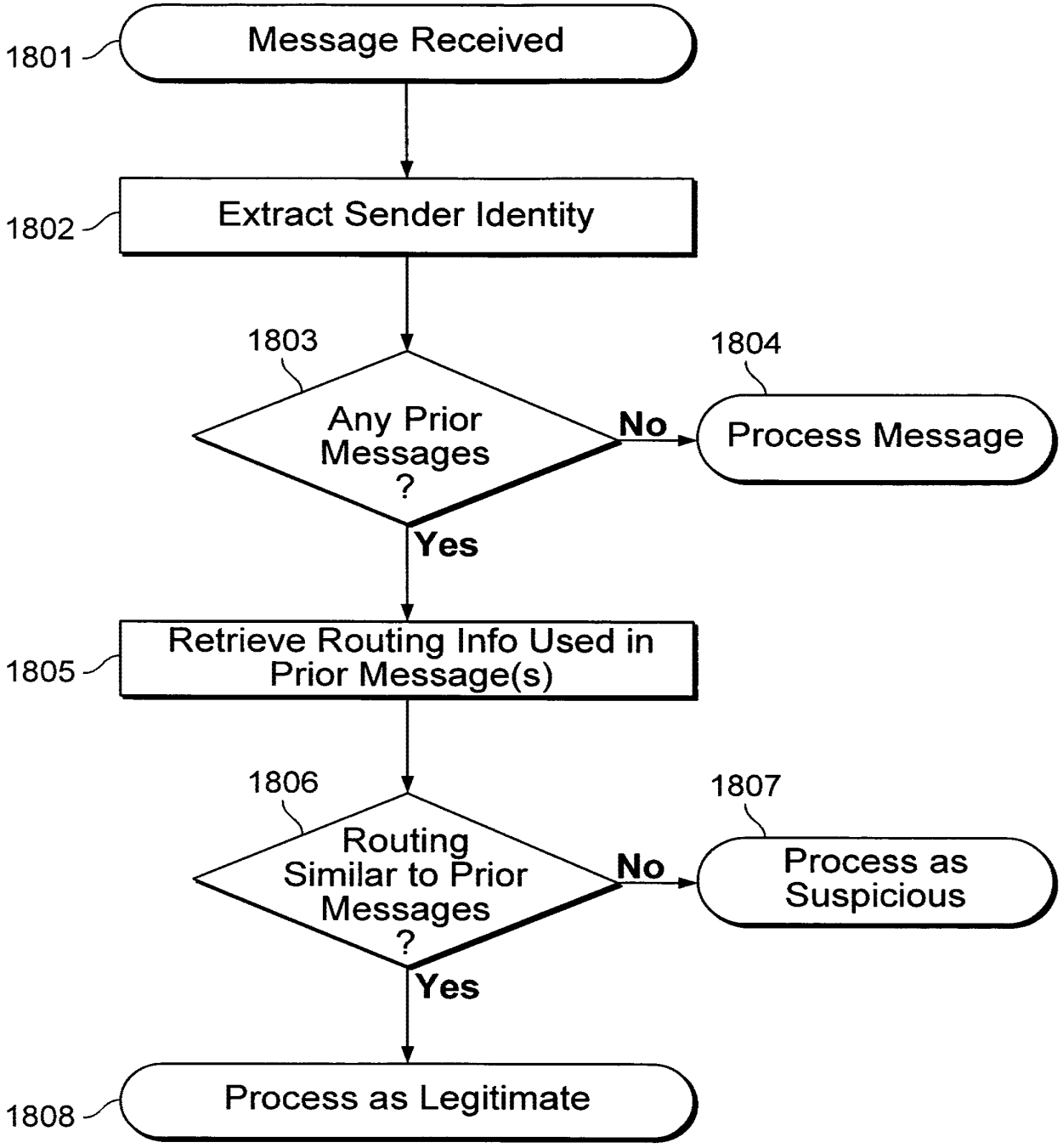

1801
Message Received
1802
Extract Sender Identity
1803
Any Prior Messages ?
No
1804
Process Message
Yes
1805
Retrieve Routing Info Used in Prior Message(s)
1806
Routing Similar to Prior Messages ?
No
1807
Process as Suspicious
Yes
1808
Process as Legitimate

FIG. 18

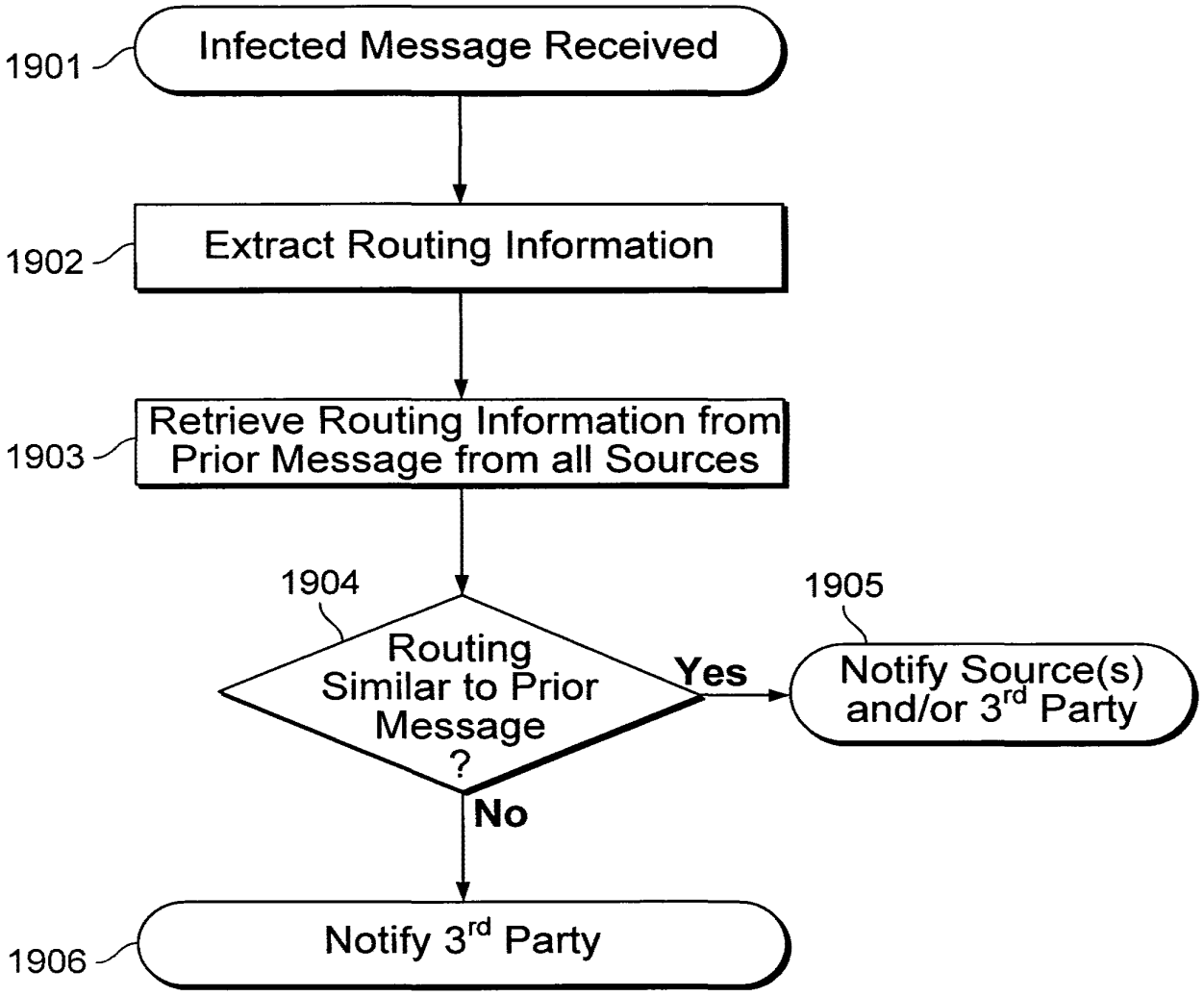

1901
Infected Message Received
1902
Extract Routing Information
1903
Retrieve Routing Information from Prior Message from all Sources
1904
Routing Similar to Prior Message ?
Yes
1905
Notify Source(s) and/or 3rd Party
No
1906
Notify 3rd Party

FIG. 19A

25/25

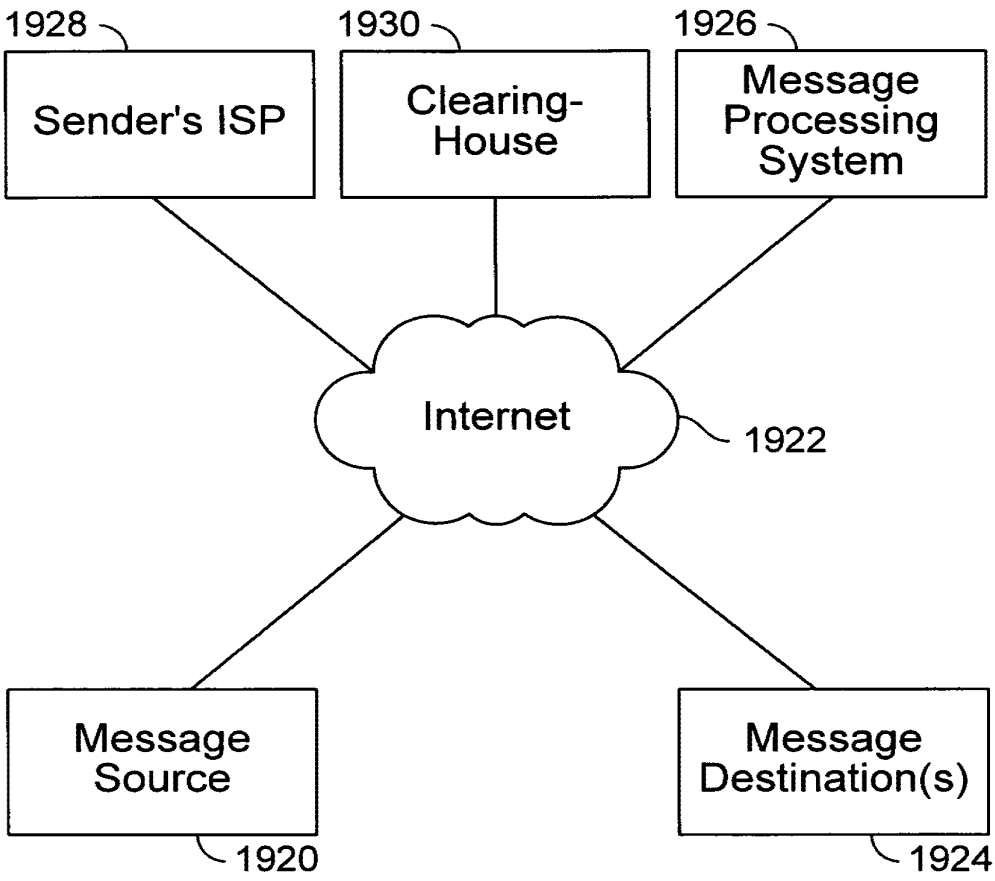

1928
Sender's ISP
1930
Clearing-House
1926
Message Processing System
Internet
1922
Message Source
1920
Message Destination(s)
1924

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
11/237,004	09/27/2005	James A. Roskind	RAD2P003

CONFIRMATION NO. 6024

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FORMALITIES LETTER

Date Mailed: 12/23/2005

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- 3d, 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.

H. Hume

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382

092705
19638 U.S. PTO

UTILITY PATENT APPLICATION TRANSMITTAL

Under Small Entity Status

(New Nonprovisional Applications Under 37 CFR § 1.53(b))

Attorney Docket No. RAD2P003

113211 U.S. PTO
11/237004
092705

TO THE COMMISSIONER FOR PATENTS:

Transmitted herewith is the patent application of ( ) application identifier or (X) first named inventor, James A. Roskind, entitled DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS, 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 $600.00 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	17	0	$ 25.00	$ 0.00
Independent Claims	4	1	$100.00	$100.00
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	**$ 600.00**

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. RAD2P003).

Respectfully submitted,

By: William J. James

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.: EV323820143US

Date of Deposit: September 27, 2005

Attorney Docket No. RAD2P003

APPLICATION FOR UNITED STATES PATENT

DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

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

DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

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] Unwanted and/or malicious network communications, such as spam, phishing, worm propagation, etc., hamper productivity and the use and enjoyment of computer and network resources by end users, burden affected networks with unauthorized and/or undesired traffic, and expose recipients to the risk of theft, fraud, etc. Current technologies for dealing with such unauthorized and/or unwanted communications focus on filtering messages at a point in the communication path close to the recipient system, such as anti-spam and/or other security software installed on the destination host and/or a local mail (or other messaging) server to which communications to the destination host are directed for delivery to the destination host, e.g., by detecting messages sent by blacklisted senders and/or messages containing header or other content that indicates the message is suspicious. While this approach can be an effective way to protect an individual host or a group of destination hosts served by a local server, it does not address the network congestion problem and leaves vulnerable hosts not protected by destination (or destination mail or messaging server) based filtering software. In addition, in many cases an attacker causes each of one or more compromised hosts to send multiple instances of a malicious communication, often simultaneously or nearly so, magnifying the effect on the network. Therefore, there is a need for an effective way to

intercept and take corrective action with respect to unauthorized, unwanted, and/or otherwise malicious electronic mail and/or other network communications that better protects the network and provides protection to destination hosts that are not protected by destination or destination mail or messaging server based filtering software.

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.

[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.

[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.

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] Analyzing routing information to identify and intercept unauthorized, unwanted, and/or otherwise malicious communications is disclosed. In some embodiments, routing information associated with a message currently being processed is checked against corresponding information associated with a message from the same source that was processed previously. In some embodiments, a message processing system that handled and/or otherwise has access to routing information for both messages

performs the check, such as a network messaging and/or access service provider with which the sender is associated, performs the check. If the routing information for the current message does not match the corresponding information observed in the previous message, responsive action is taken.

[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, 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 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 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, 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 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 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 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) 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 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 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 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 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 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, 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 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, 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 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 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 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 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 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 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 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 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 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:

CLAIMS

1. A method for identifying a message as suspicious, comprising:

extracting from a received message an identity of a sender of the received message;

retrieving a prior routing data associated with a prior message received previously from the sender; and

identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message.

2. A method as recited in claim 1, further including processing the received message normally if it is determined that no prior routing data associated with the sender is available.

3. A method as recited in claim 1, wherein the prior routing data includes data extracted from a header portion of the prior message.

4. A method as recited in claim 1, wherein the prior routing data includes an IP address retrieved during a prior instant messaging session.

5. A method as recited in claim 1, wherein identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message includes:

determining a first source IP address associated with the prior message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

6. A system for identifying a message as suspicious, comprising:

a processor configured to:

extract from a received message an identity of a sender of the received message;

retrieve a prior routing data associated with a prior message received previously from the sender; and

identify the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message; and

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

7. A system as recited in claim 6, wherein the processor is further configured to process the received message normally if it is determined that no prior routing data associated with the sender is available.

8. A system as recited in claim 6, wherein the prior routing data includes data extracted from a header portion of the prior message.

9. A system as recited in claim 6, wherein the prior routing data includes an IP address retrieved during a prior instant messaging session.

10. A system as recited in claim 6, wherein the processor is configured to identify the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message at least in part by:

determining a first source IP address associated with the prior message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

11. A computer program product for identifying a message as suspicious, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

extracting from a received message an identity of a sender of the received message;

retrieving a prior routing data associated with a prior message received previously from the sender; and

identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message.

12. A computer program product as recited in claim 11, the computer program product further comprising computer instructions for processing the received message normally if it is determined that no prior routing data associated with the sender is available.

13. A computer program product as recited in claim 11, wherein the prior routing data includes data extracted from a header portion of the prior message.

14. A computer program product as recited in claim 11, wherein the prior routing data includes an IP address retrieved during a prior instant messaging session.

15. A computer program product as recited in claim 11, wherein identifying the received message as suspicious if the prior routing data is different than a corresponding current routing data associated with the received message in a way that indicates the received message was received from a different originating source than the prior message includes:

determining a first source IP address associated with the prior message;

determining a second source IP address associated with the prior message; and

determining whether the first source IP address and the second source IP address are associated with the same geographical region.

16. A method for reporting a malicious network communication, comprising:

determining that a received network communication comprises malicious data;

extracting routing information from the received network communication;

retrieving corresponding prior routing information from a prior network communication received previously from a sender with which the received network communication is associated; and

notifying the sender that the received network communication included malicious data if a comparison of the routing information extracted from the received network communication to the prior routing information does not indicate that the received network communication and the prior network communication came from different originating sources.

17. A method as recited in claim 16, further including notifying a third party, but not the sender, if the comparison of the routing information extracted from the received network communication to the prior routing information indicates that the received network communication and the prior network communication came from different originating sources.

DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS

ABSTRACT OF THE DISCLOSURE

[0061] Analyzing routing information to identify and intercept unauthorized, unwanted, and/or otherwise malicious communications is disclosed. In some embodiments, routing information associated with a message currently being processed is checked against corresponding information associated with a message from the same source that was processed previously. In some embodiments, a message processing system that handled and/or otherwise has access to routing information for both messages performs the check, such as a network messaging and/or access service provider with which the sender is associated, performs the check. If the routing information for the current message does not match the corresponding information observed in the previous message, responsive action is taken. Using routing information to determine whether a source of an infected message should be notified is disclosed. In some embodiments, if routing information for a prior message from the source of an infected message is similar to corresponding information for the infected message, the source is notified.

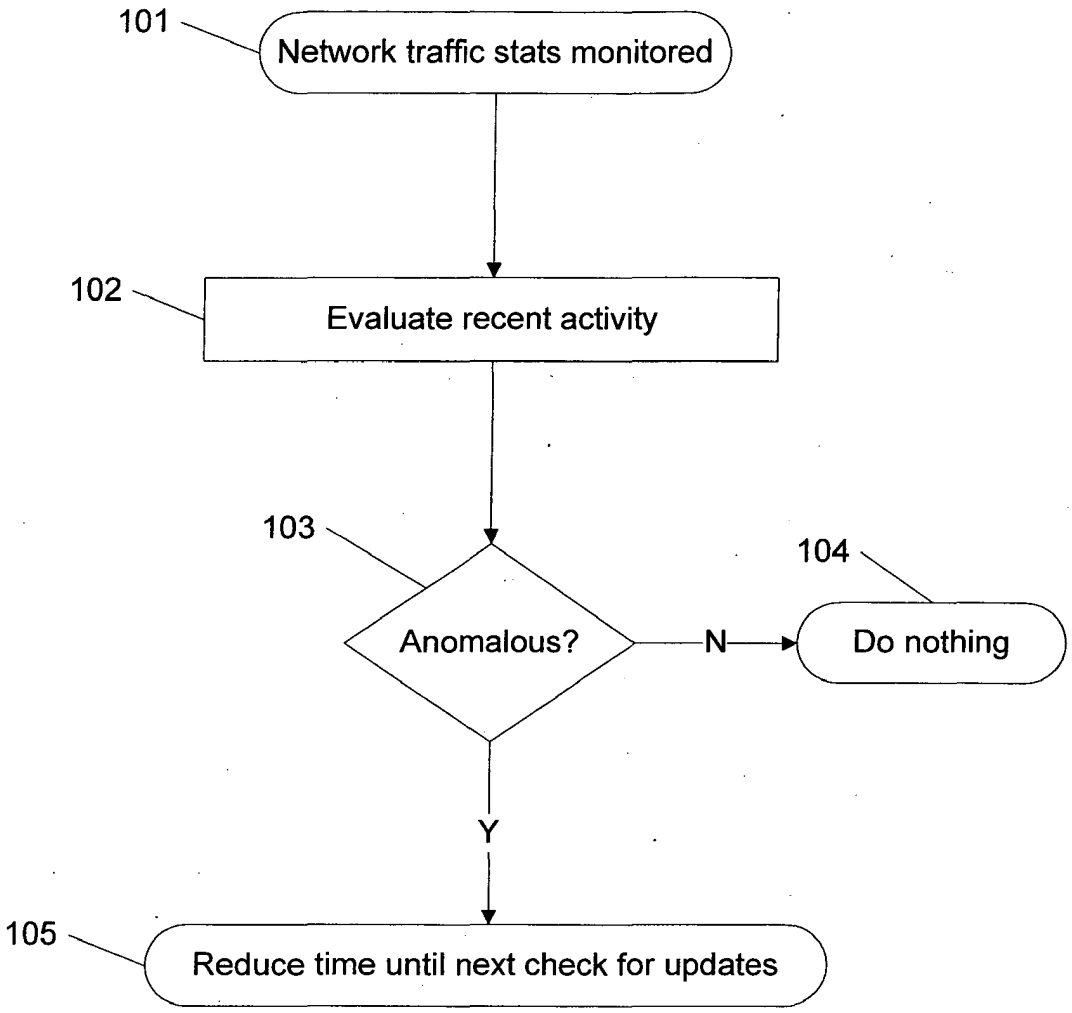


Figure 1

BEST AVAILABLE COPY

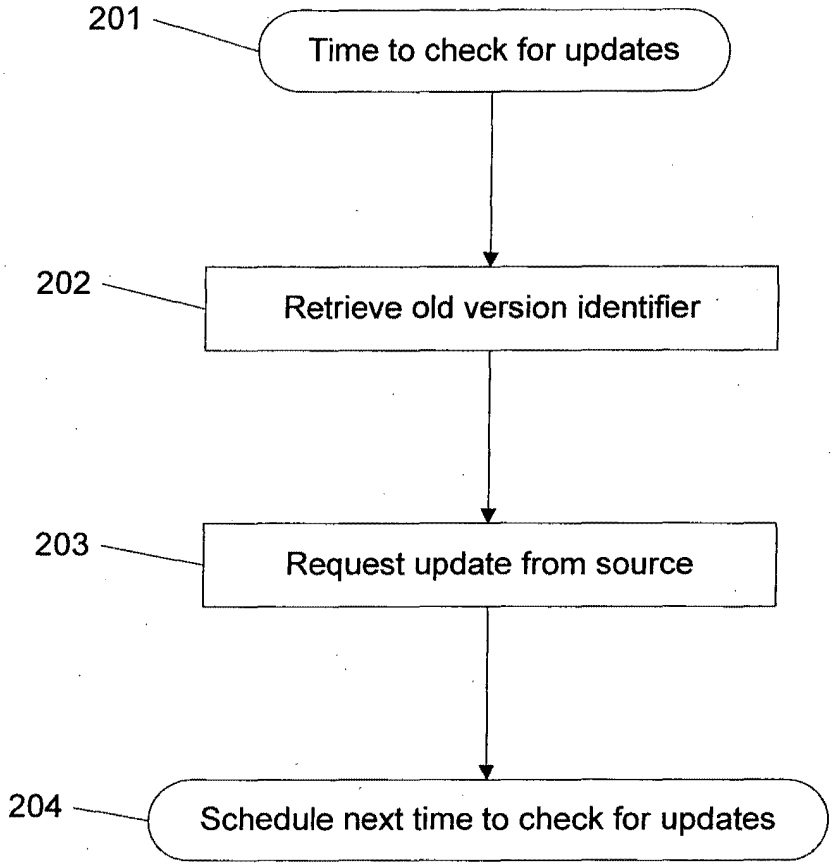

201
Time to check for updates
202
Retrieve old version identifier
203
Request update from source
204
Schedule next time to check for updates

Figure 2A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

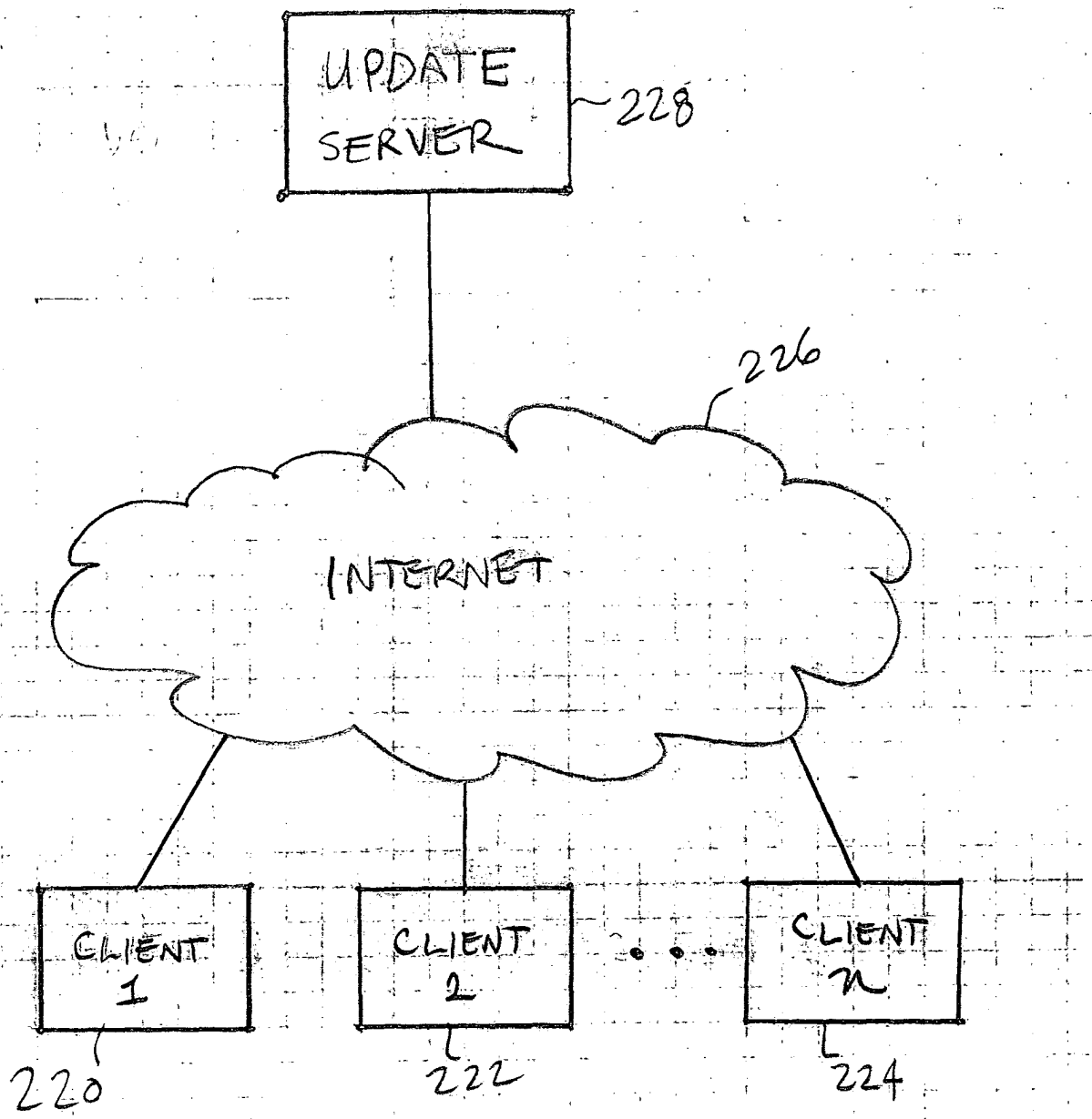


FIG. 2B

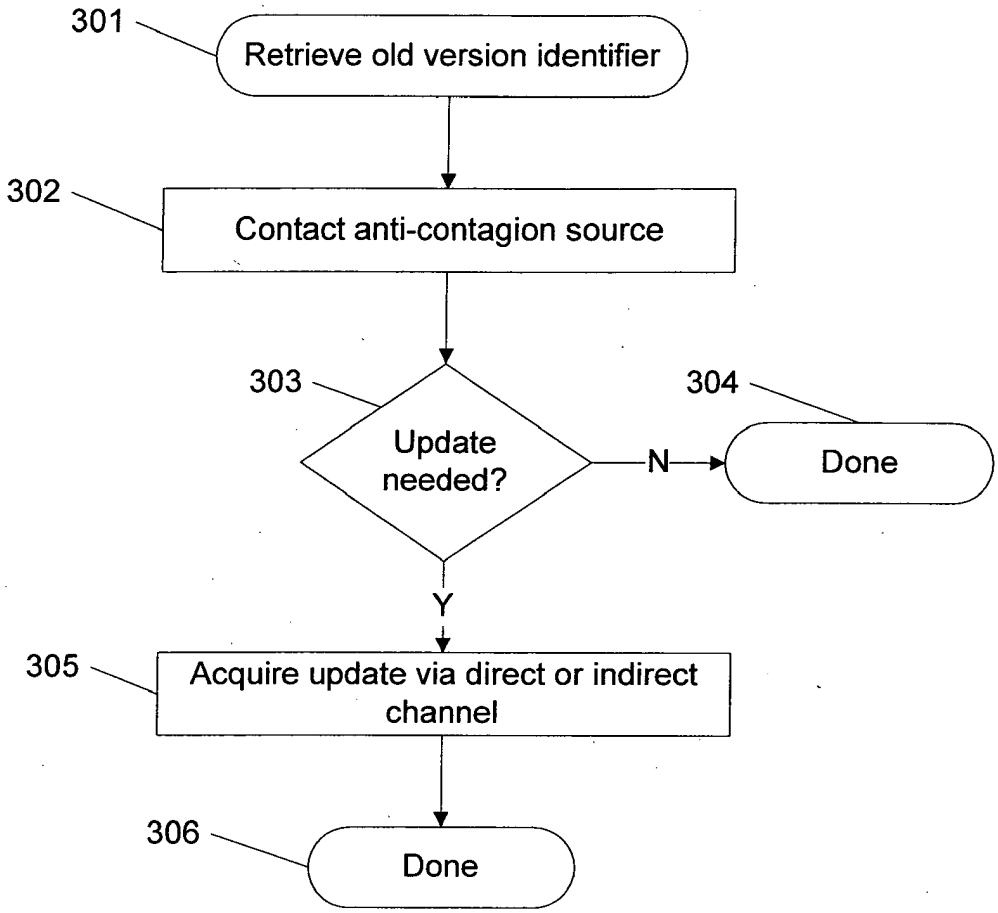

301
Retrieve old version identifier
302
Contact anti-contagion source
303
Update needed?
304
N
Done
Y
305
Acquire update via direct or indirect channel
306
Done

Figure 3A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

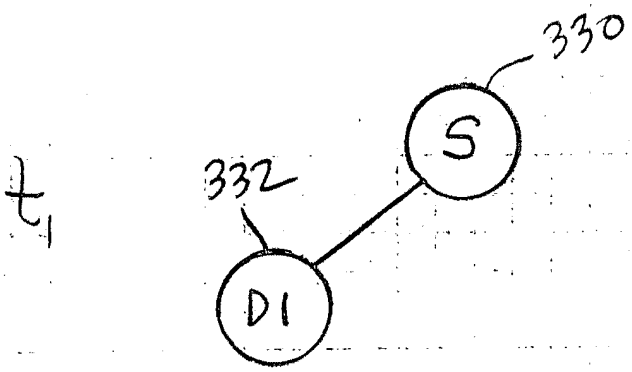


FIG. 3B

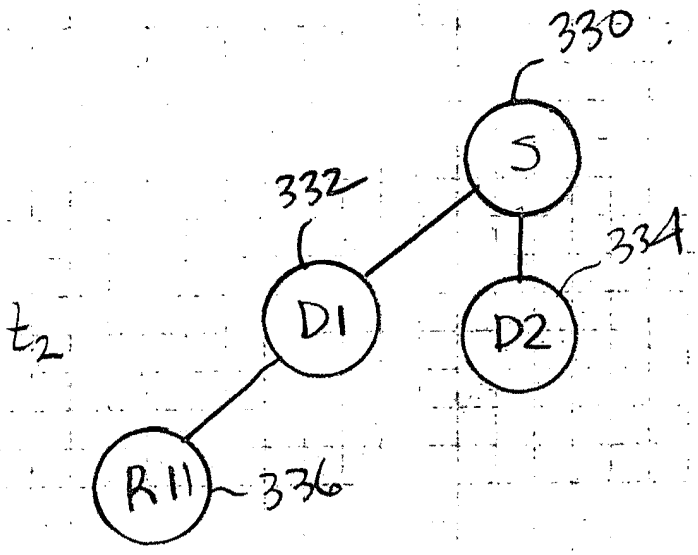


FIG. 3C

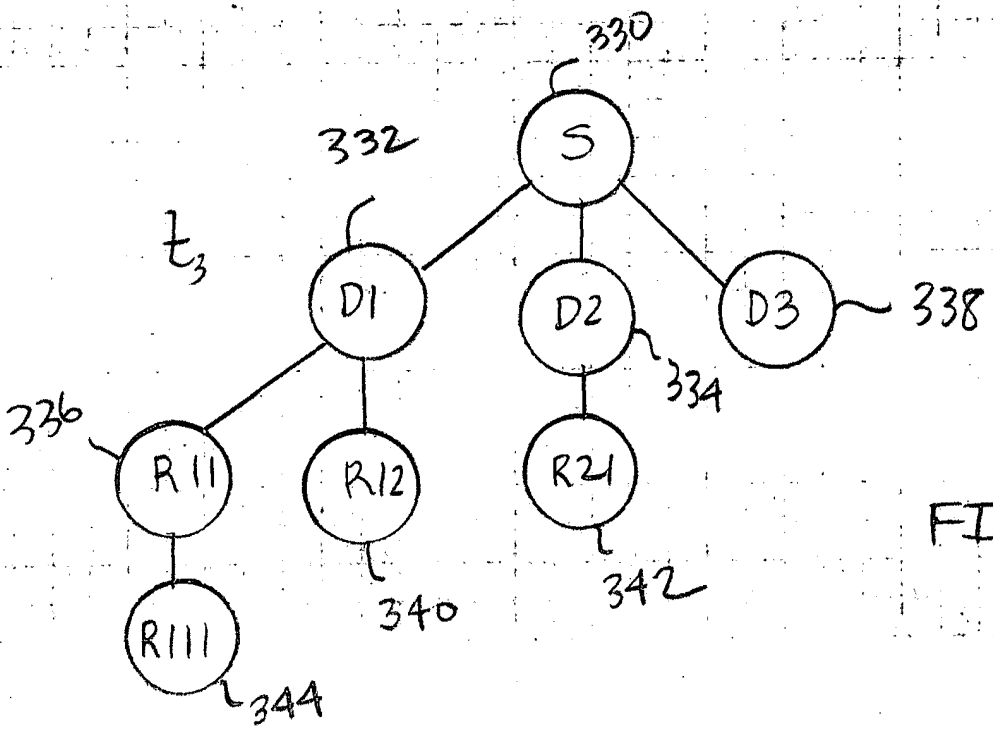


FIG. 3D

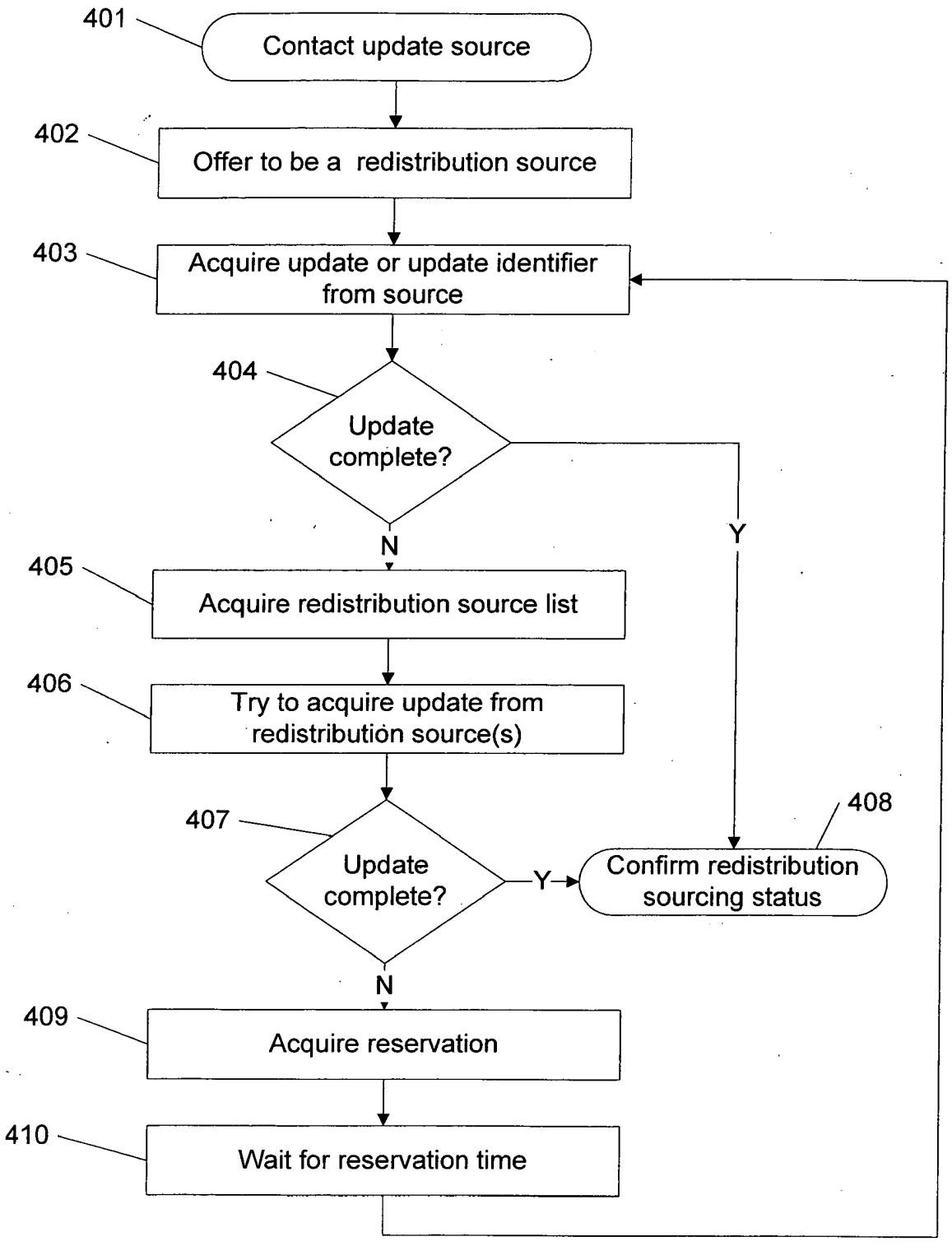

401
Contact update source
402
Offer to be a redistribution source
403
Acquire update or update identifier from source
404
Update complete?
N
Y
405
Acquire redistribution source list
406
Try to acquire update from redistribution source(s)
407
Update complete?
Y
408
Confirm redistribution sourcing status
N
409
Acquire reservation
410
Wait for reservation time

Figure 4A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

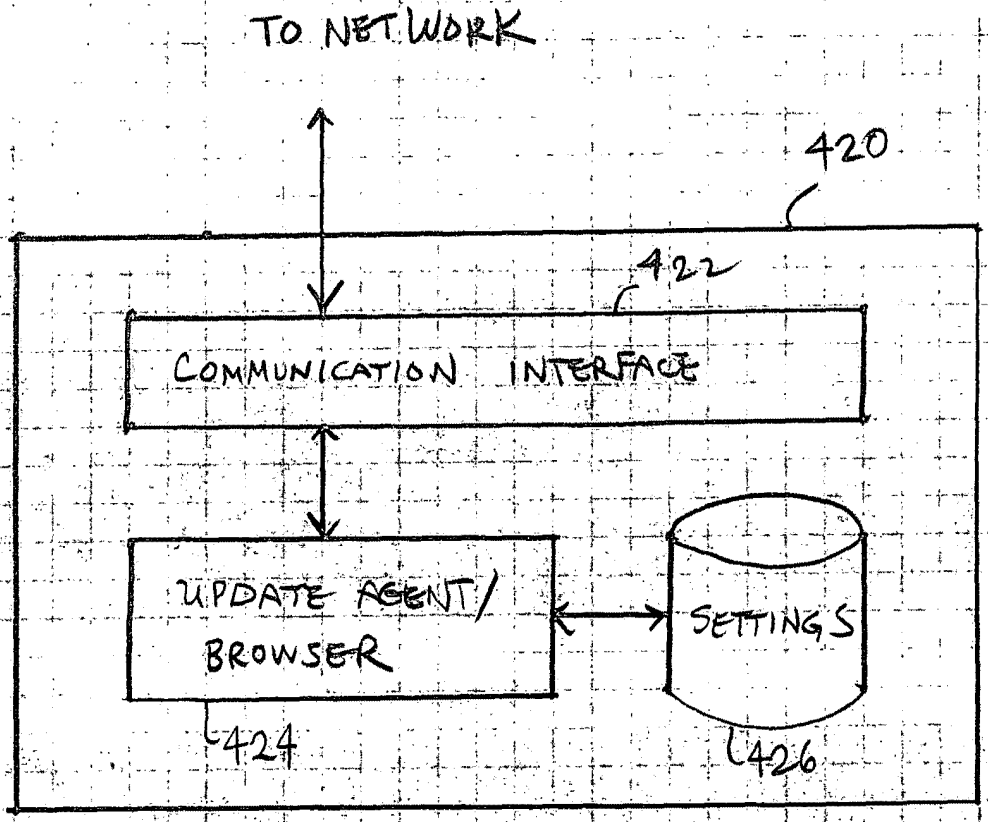


FIG. 4B

STAEDTLER® No. 937 811E
Engineer's Computation Pad

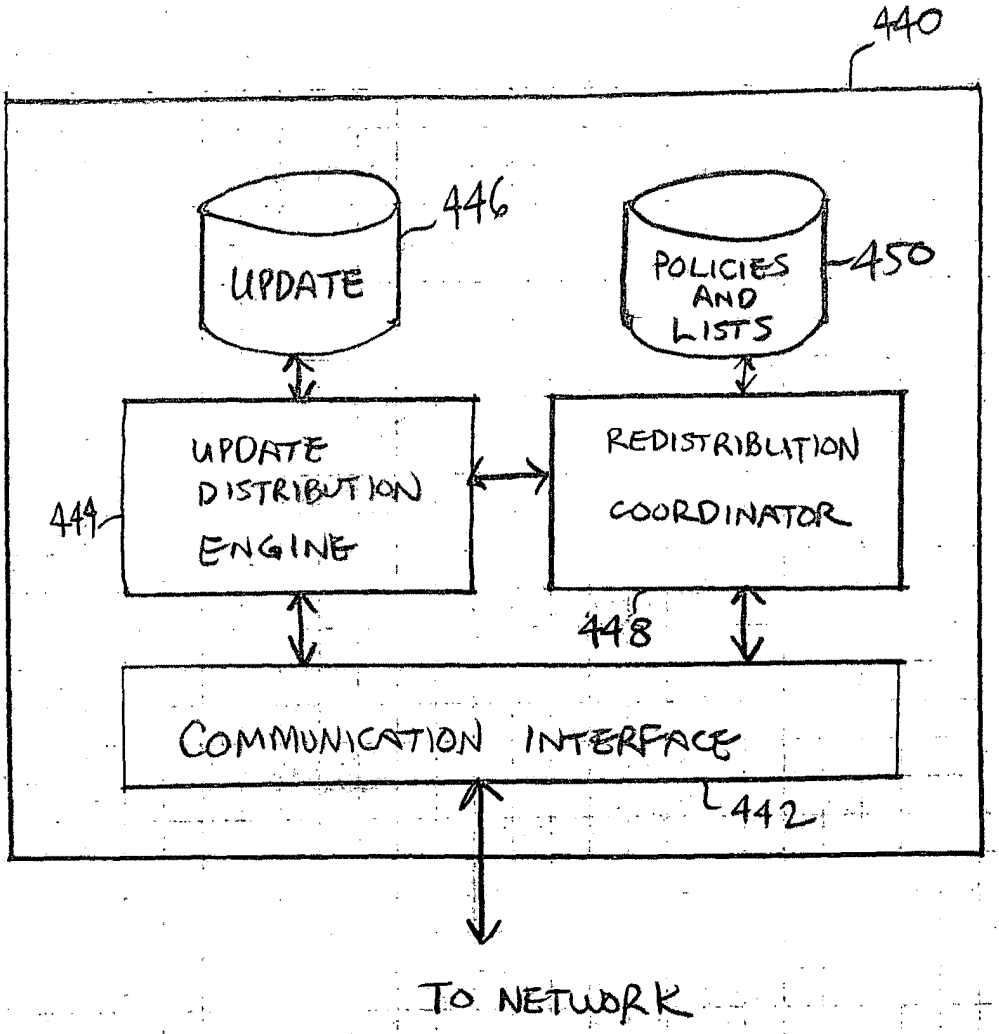


FIG. 4C

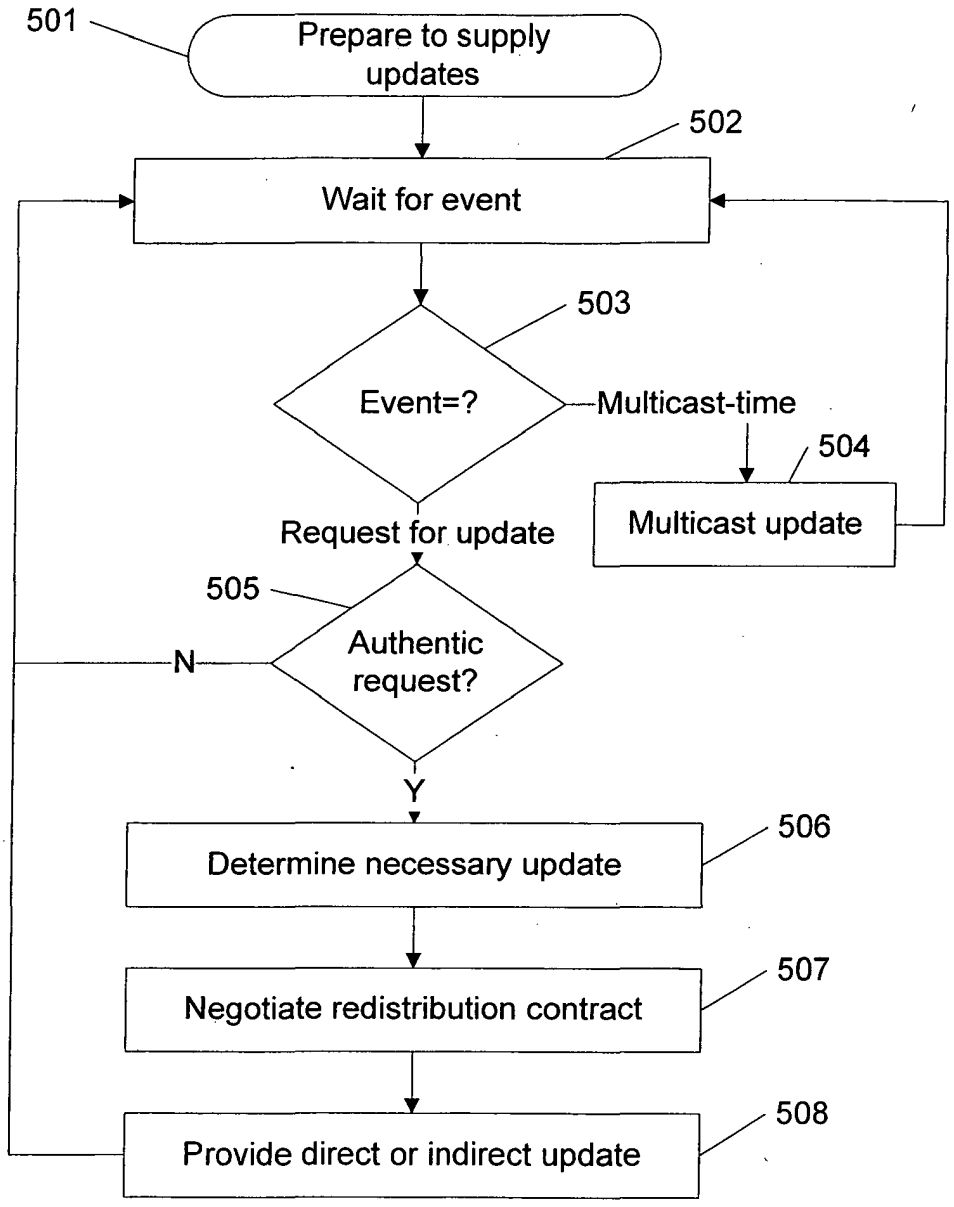

501
Prepare to supply updates
502
Wait for event
503
Event=?
Multicast-time
504
Multicast update
Request for update
505
Authentic request?
N
Y
506
Determine necessary update
507
Negotiate redistribution contract
508
Provide direct or indirect update

Figure 5

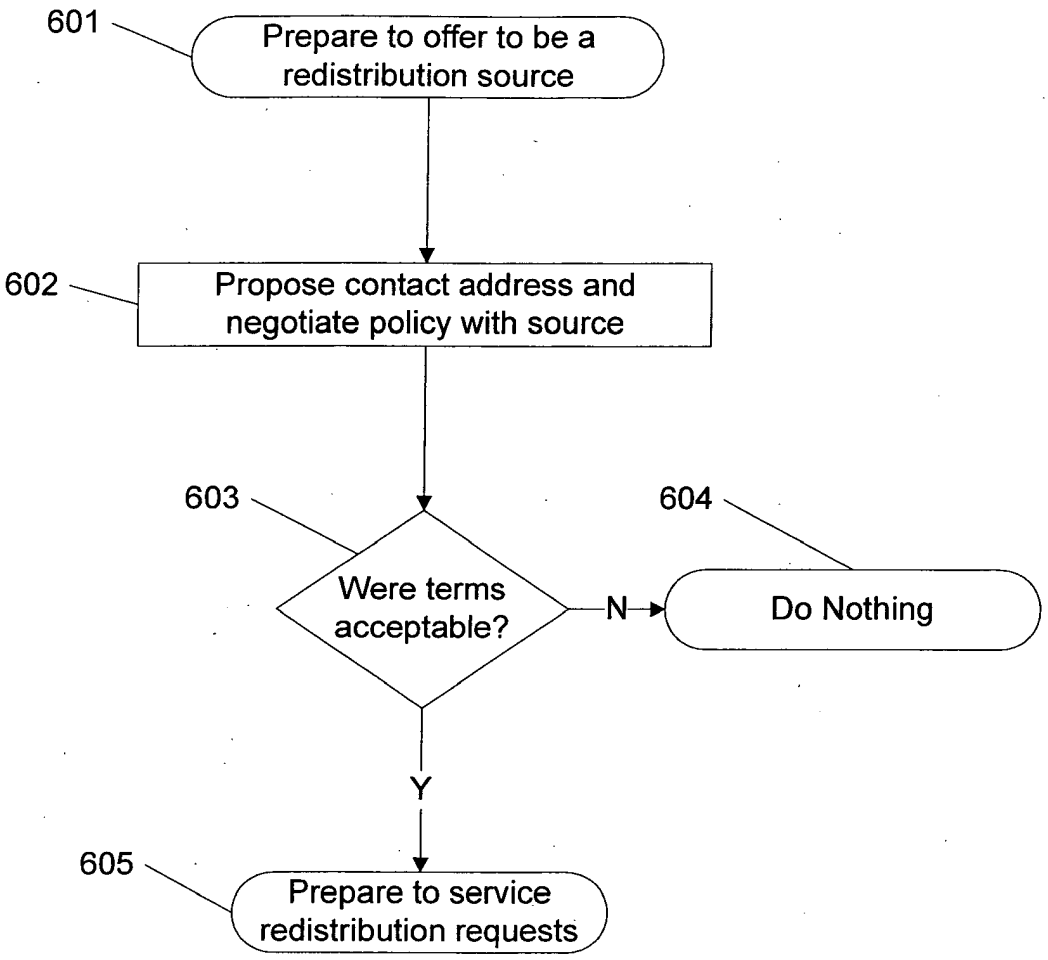

601
Prepare to offer to be a redistribution source
602
Propose contact address and negotiate policy with source
603
Were terms acceptable?
N
604
Do Nothing
Y
605
Prepare to service redistribution requests

Figure 6

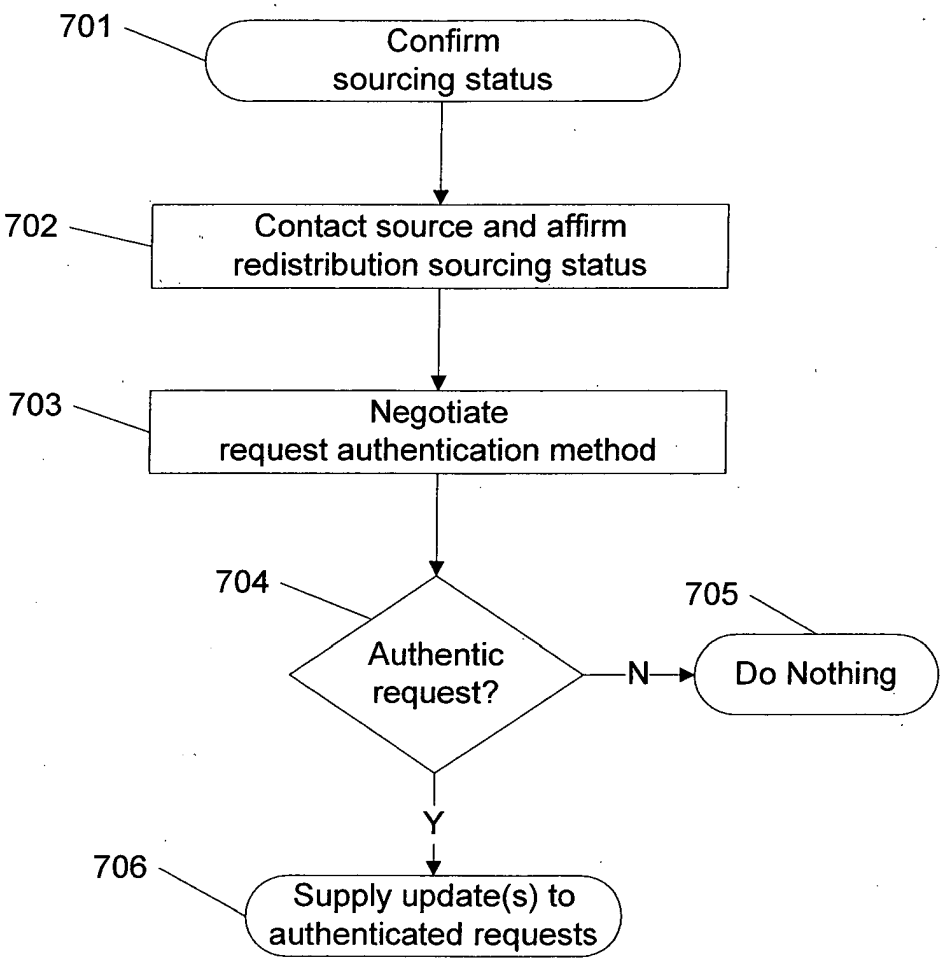

701
Confirm sourcing status
702
Contact source and affirm redistribution sourcing status
703
Negotiate request authentication method
704
Authentic request?
N
705
Do Nothing
Y
706
Supply update(s) to authenticated requests

Figure 7

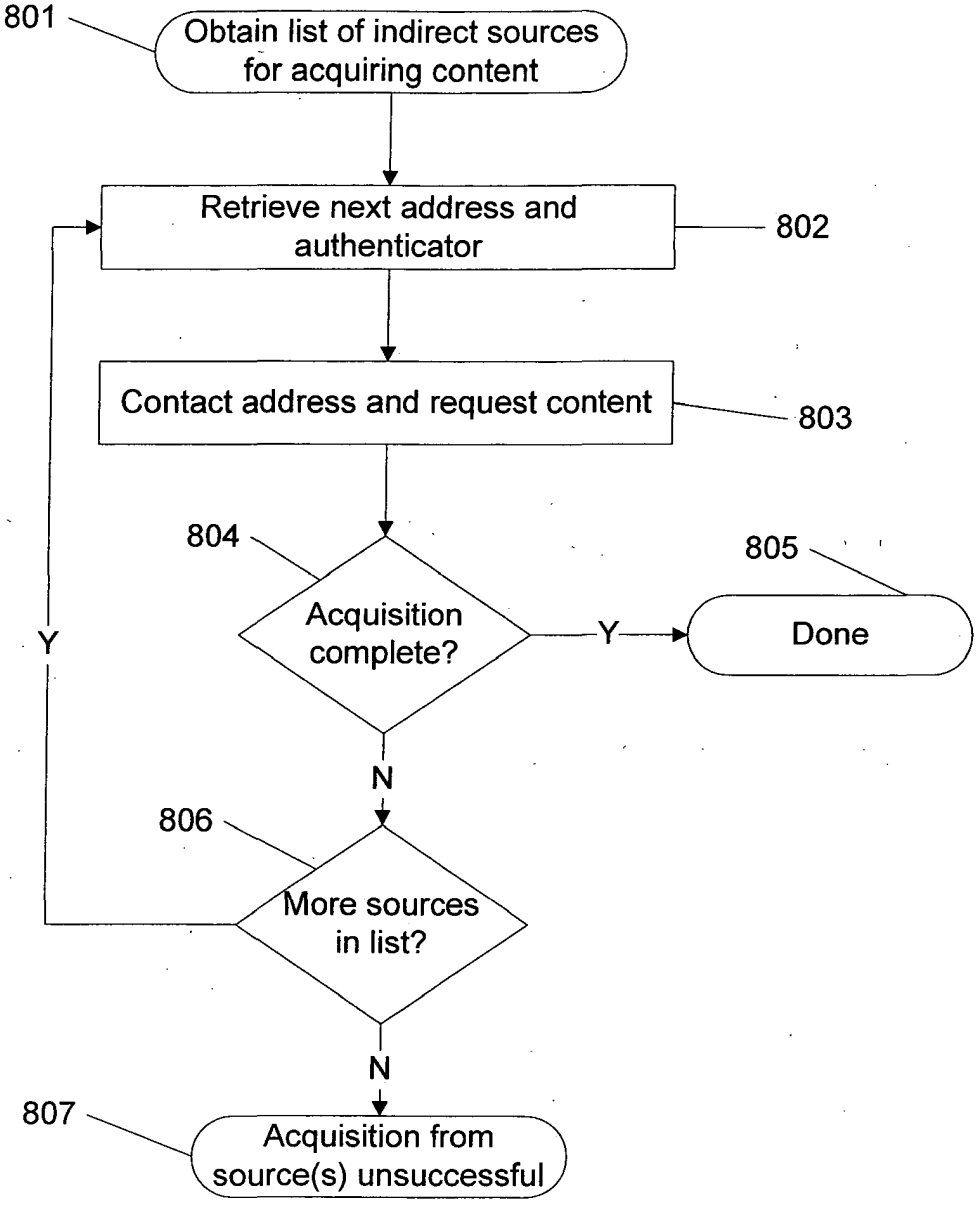

801
Obtain list of indirect sources for acquiring content
Retrieve next address and authenticator
802
Contact address and request content
803
804
Acquisition complete?
Y
805
Done
Y
N
806
More sources in list?
Y
N
807
Acquisition from source(s) unsuccessful

Figure 8

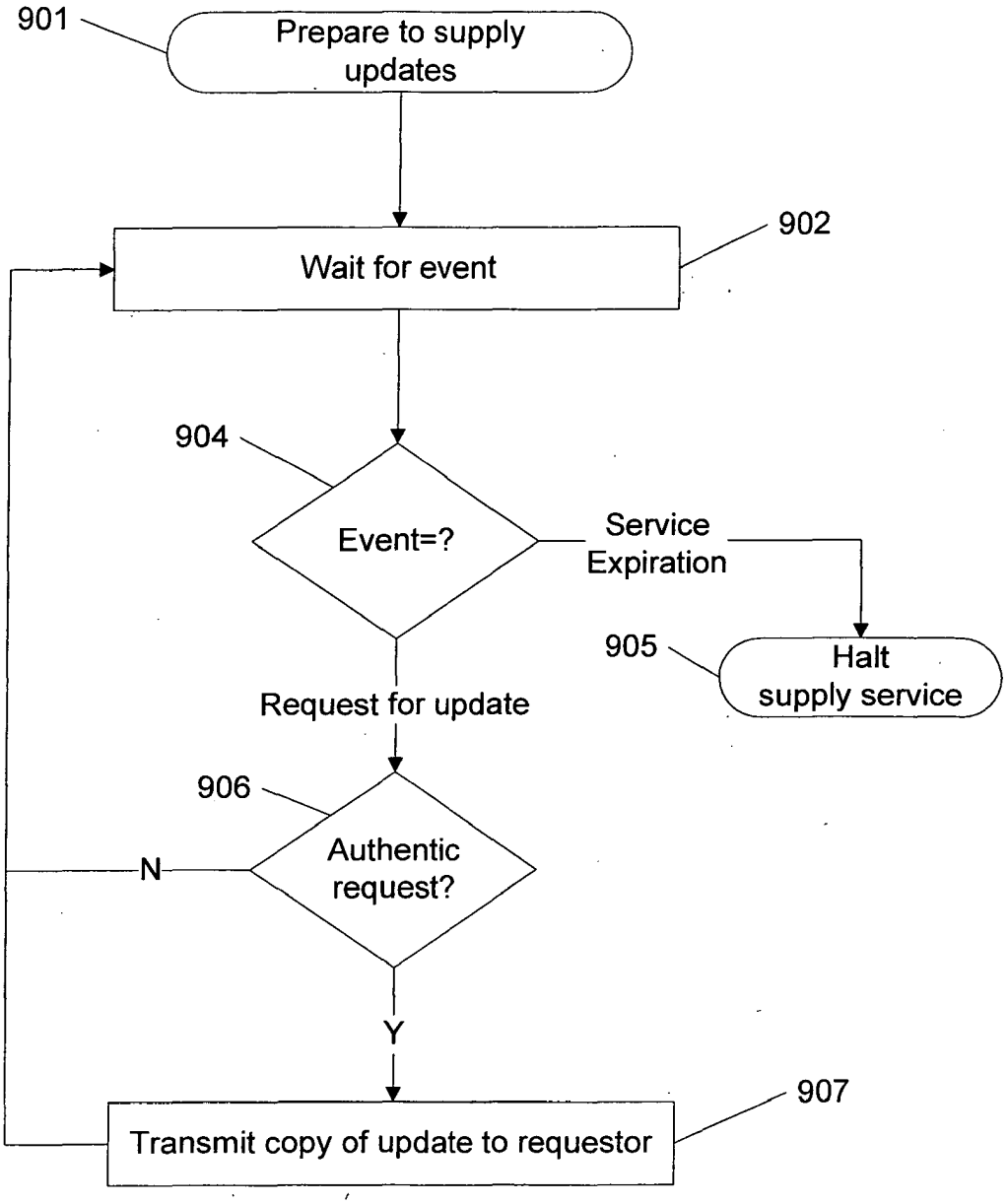

901
Prepare to supply updates
902
Wait for event
904
Event=?
Service Expiration
905
Halt supply service
Request for update
906
Authentic request?
N
Y
907
Transmit copy of update to requestor

Figure 9

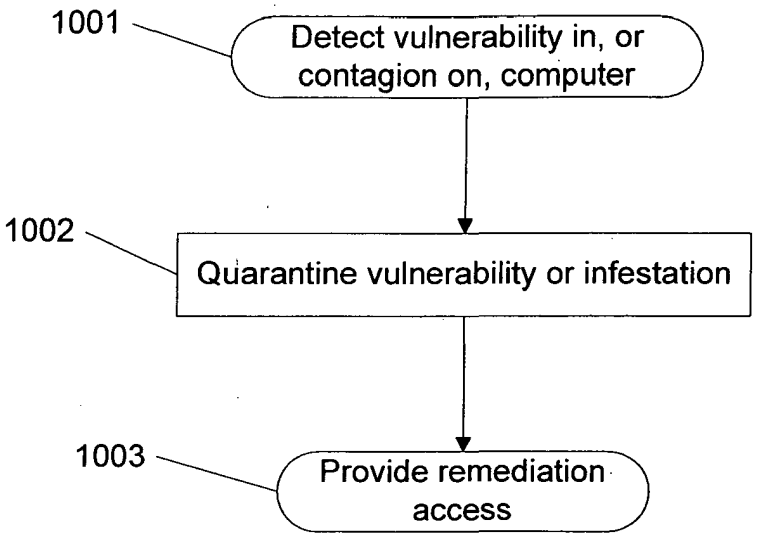

1001
Detect vulnerability in, or contagion on, computer
1002
Quarantine vulnerability or infestation
1003
Provide remediation access

Figure 10A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

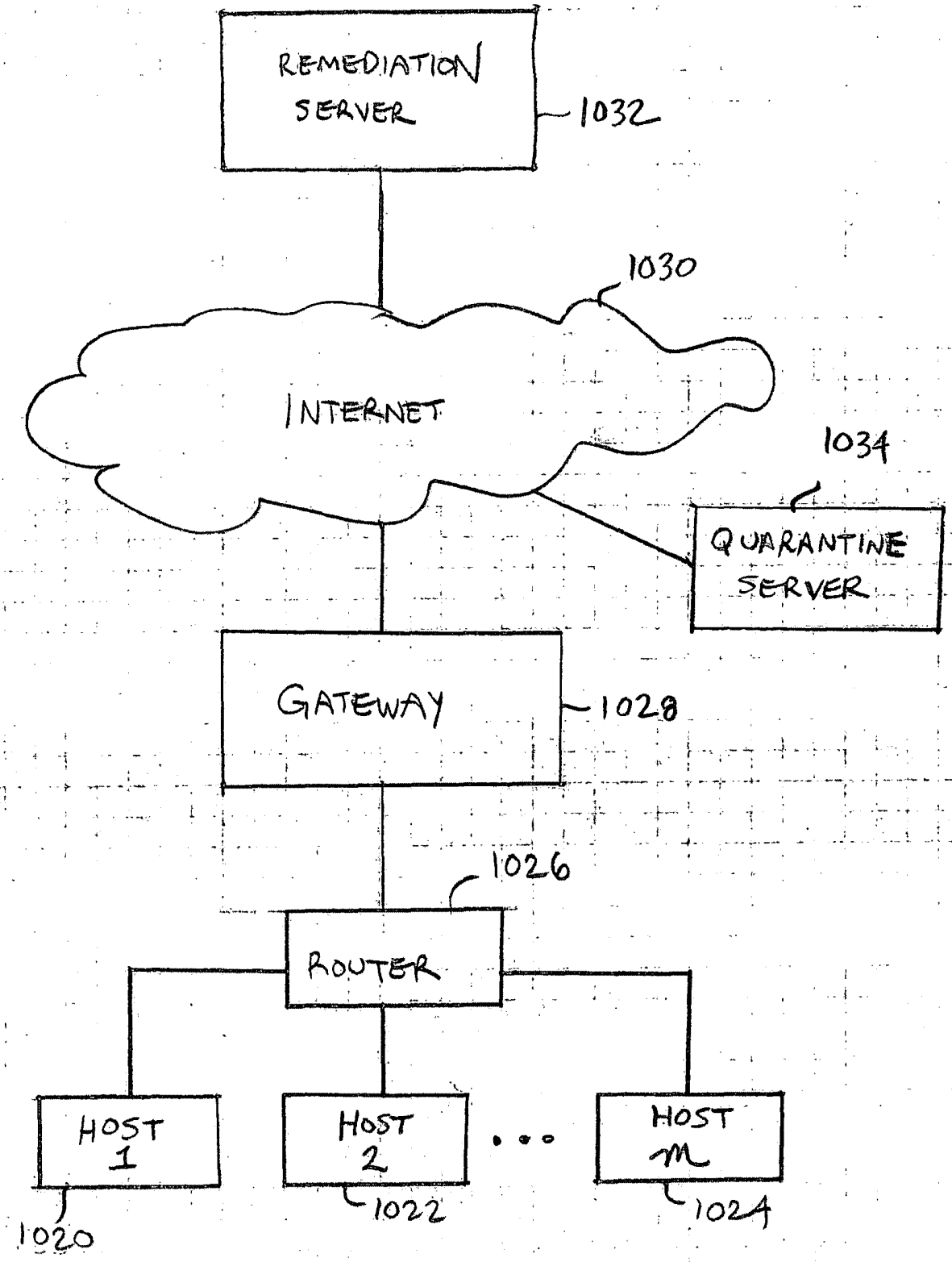


FIG. 10B

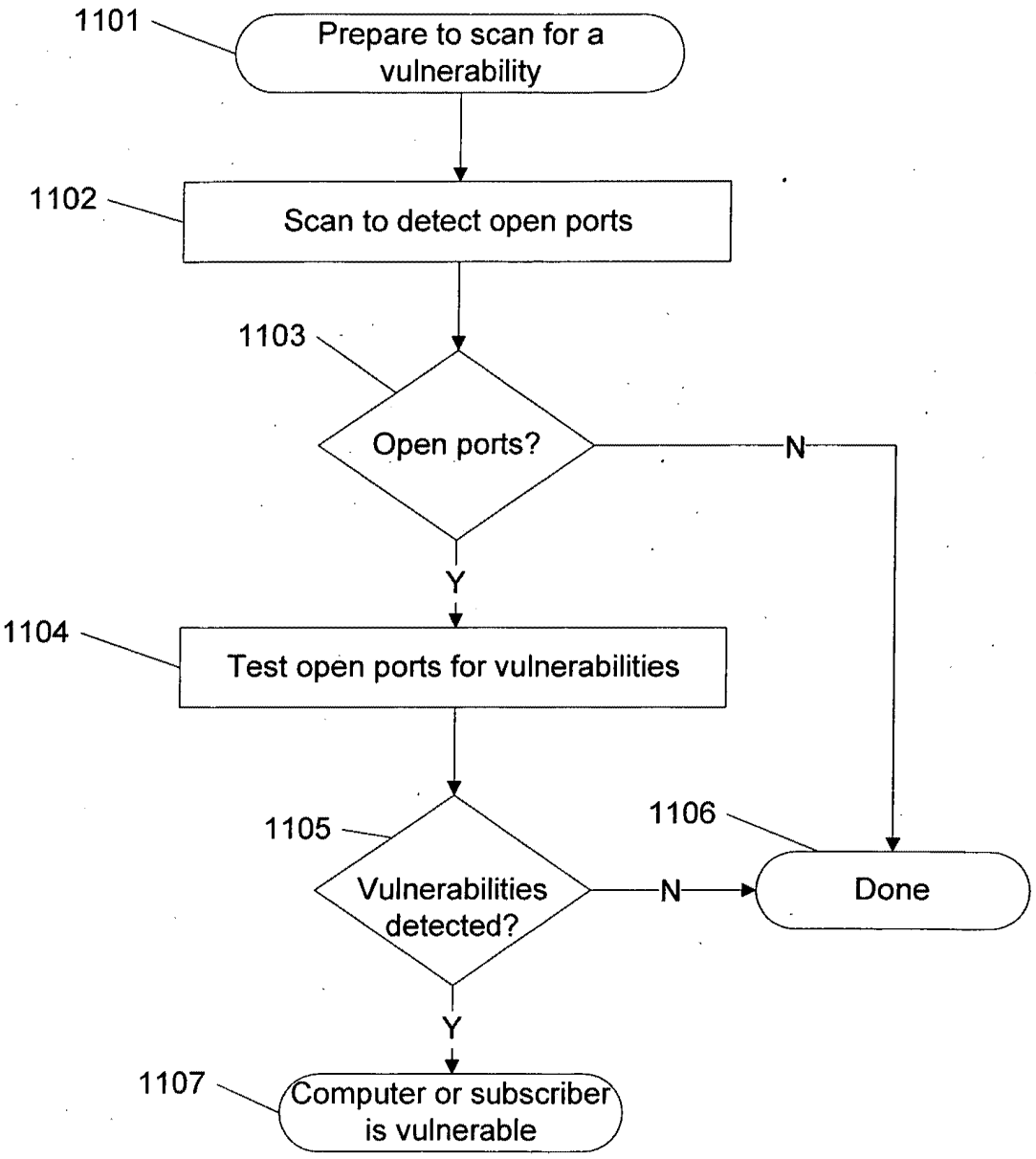

1101
Prepare to scan for a vulnerability
1102
Scan to detect open ports
1103
Open ports?
N
Y
1104
Test open ports for vulnerabilities
1105
Vulnerabilities detected?
N
1106
Done
Y
1107
Computer or subscriber is vulnerable

Figure 11

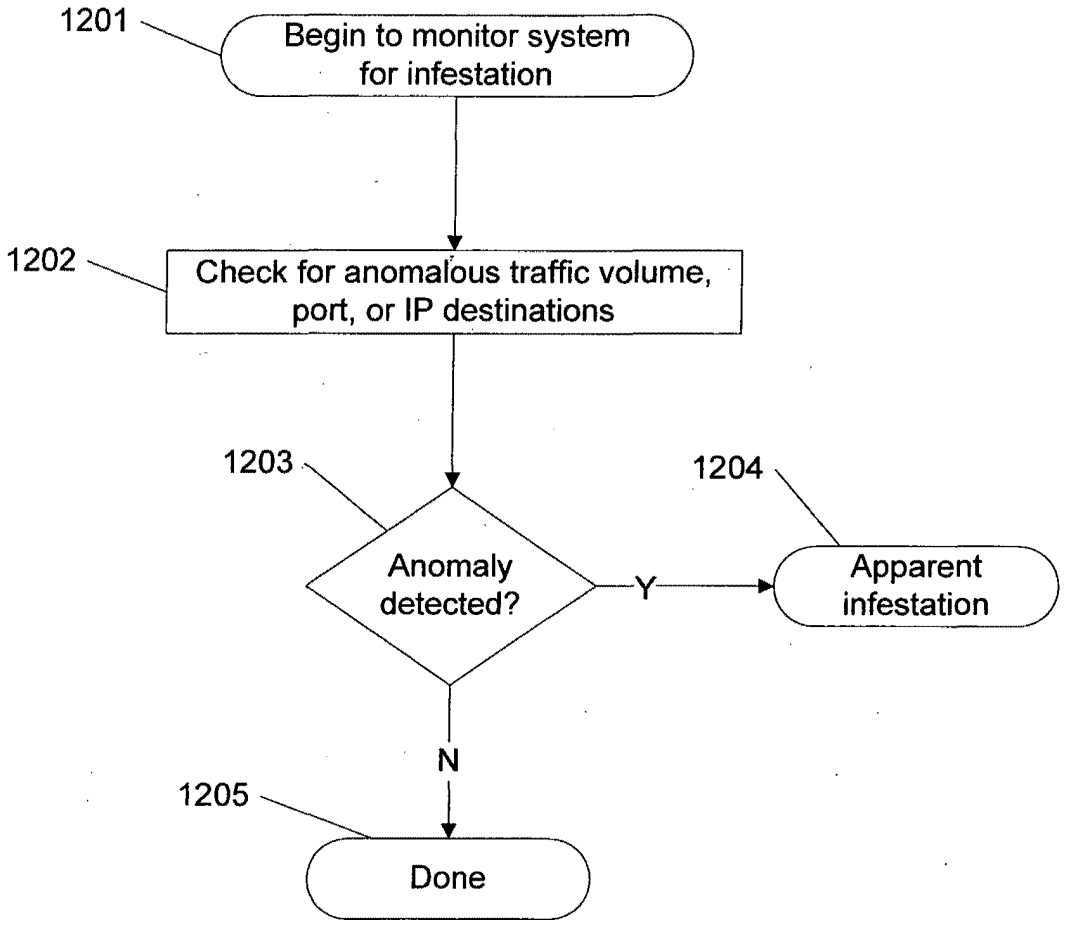

1201
Begin to monitor system for infestation
1202
Check for anomalous traffic volume, port, or IP destinations
1203
Anomaly detected?
Y
1204
Apparent infestation
N
1205
Done

Figure 12

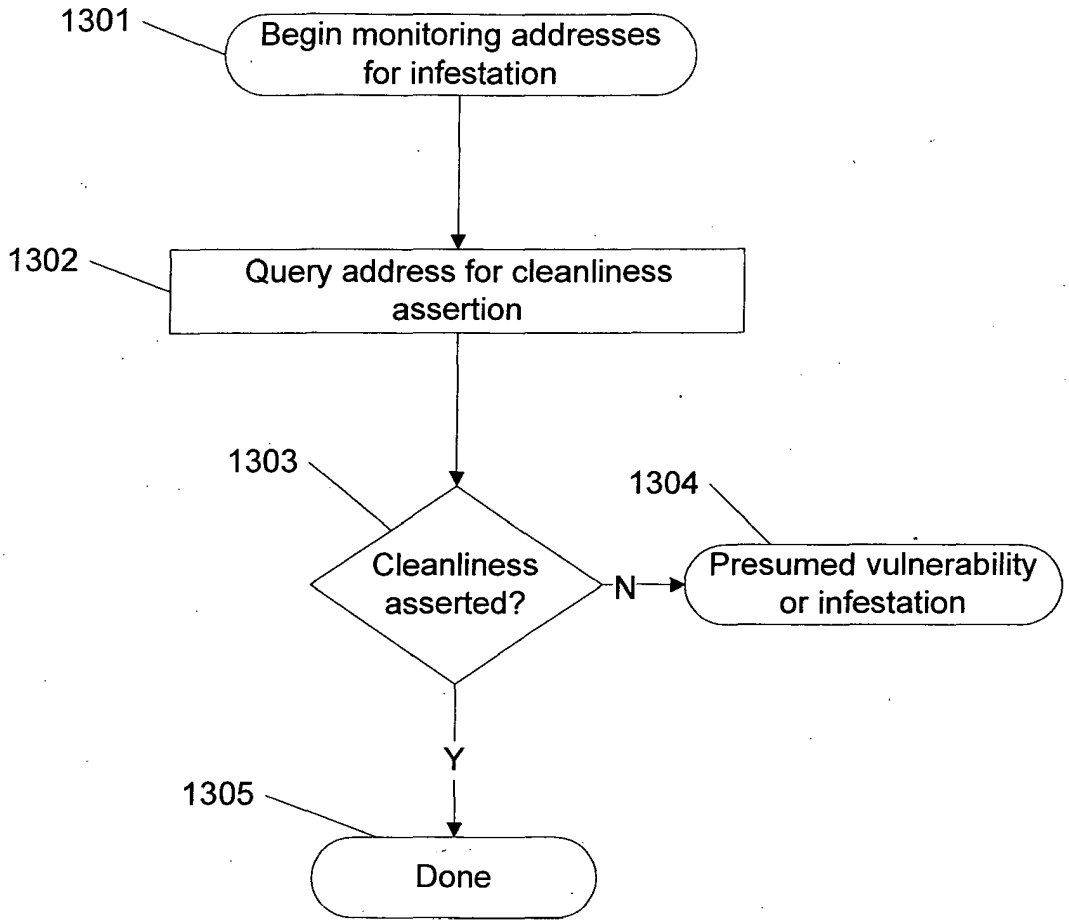

1301
Begin monitoring addresses for infestation
1302
Query address for cleanliness assertion
1303
Cleanliness asserted?
1304
N
Presumed vulnerability or infestation
Y
1305
Done

Figure 13

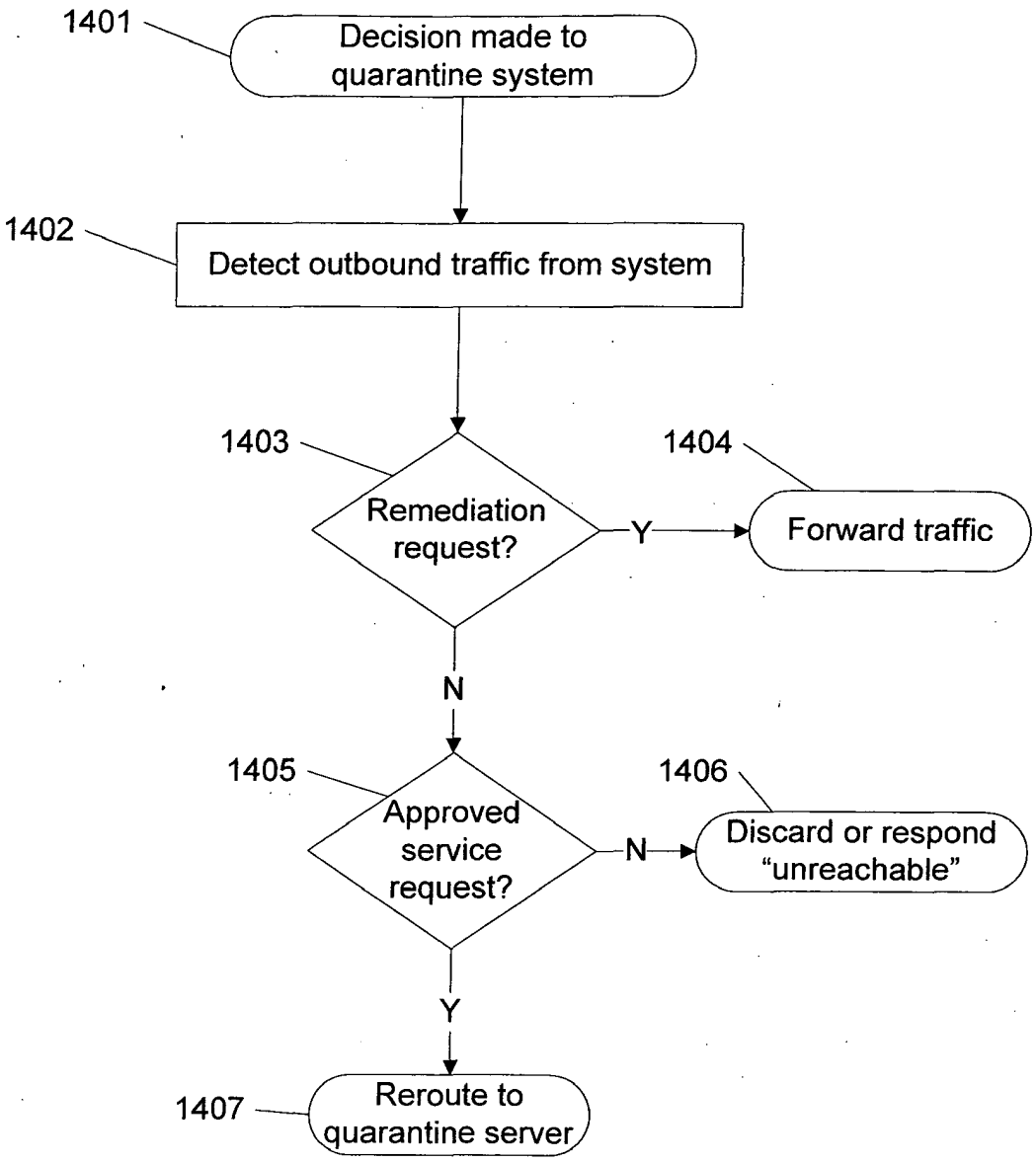

1401
Decision made to quarantine system
1402
Detect outbound traffic from system
1403
Remediation request?
Y
1404
Forward traffic
N
1405
Approved service request?
N
1406
Discard or respond "unreachable"
Y
1407
Reroute to quarantine server

Figure 14

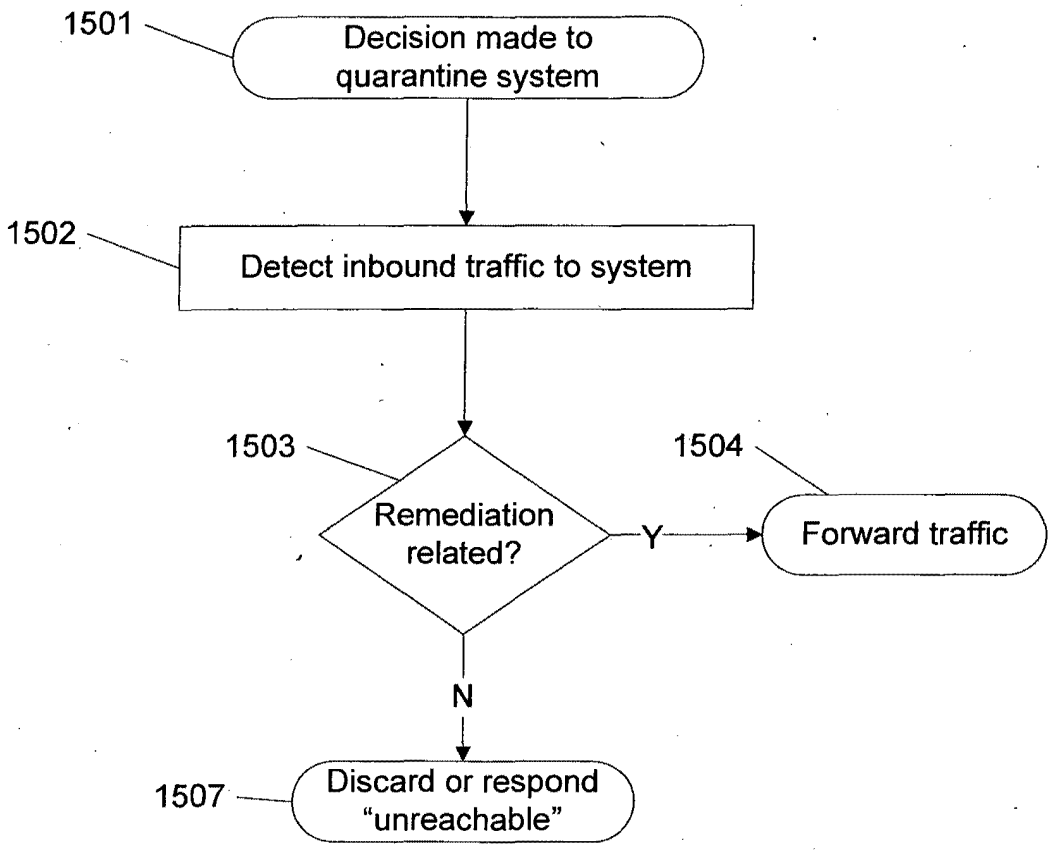

1501
Decision made to quarantine system
1502
Detect inbound traffic to system
1503
Remediation related?
Y
1504
Forward traffic
N
1507
Discard or respond "unreachable"

Figure 15

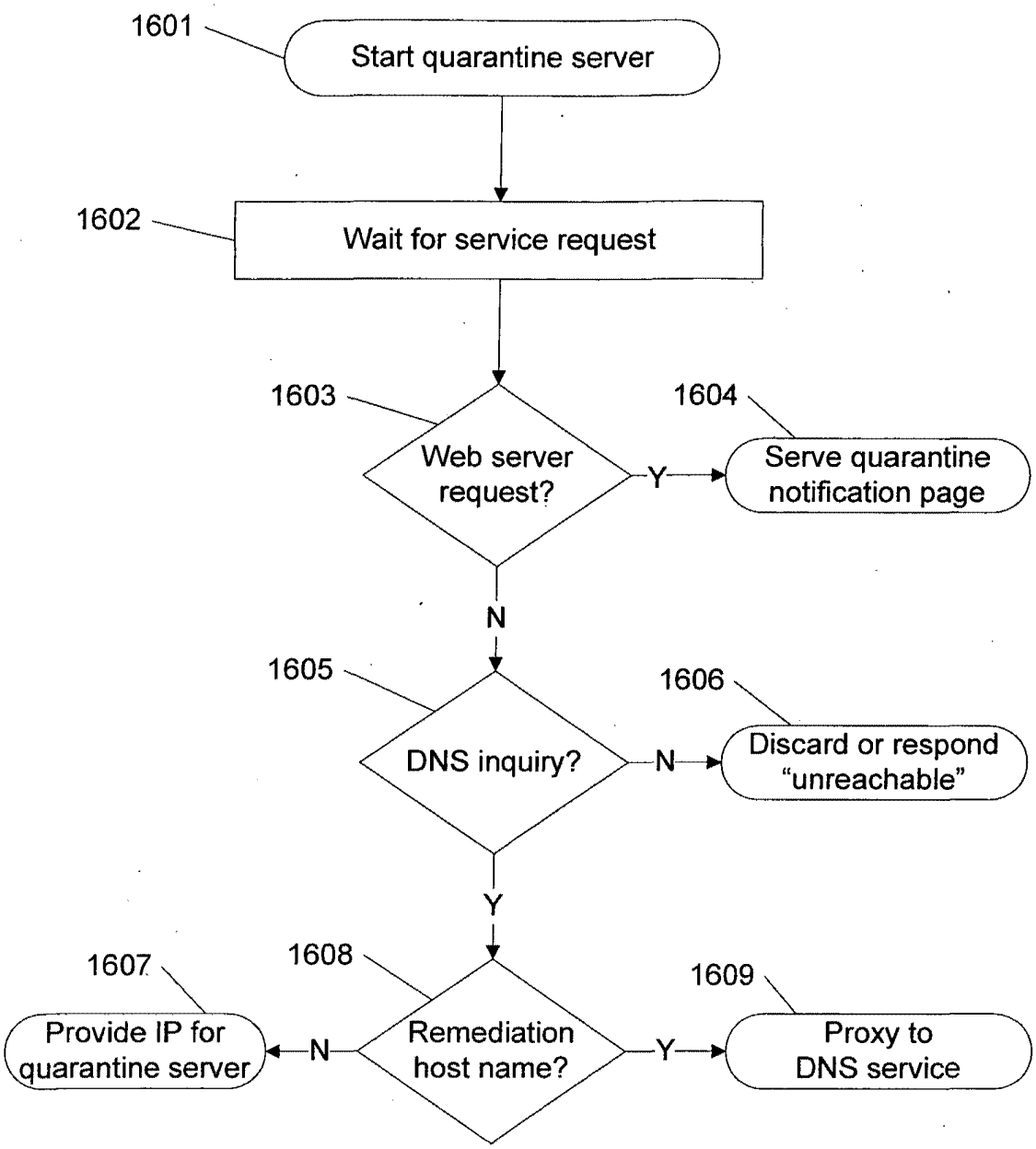

1601
Start quarantine server
1602
Wait for service request
1603
Web server request?
Y
1604
Serve quarantine notification page
N
1605
DNS inquiry?
N
1606
Discard or respond "unreachable"
Y
1607
Provide IP for quarantine server
N
1608
Remediation host name?
Y
1609
Proxy to DNS service

Figure 16

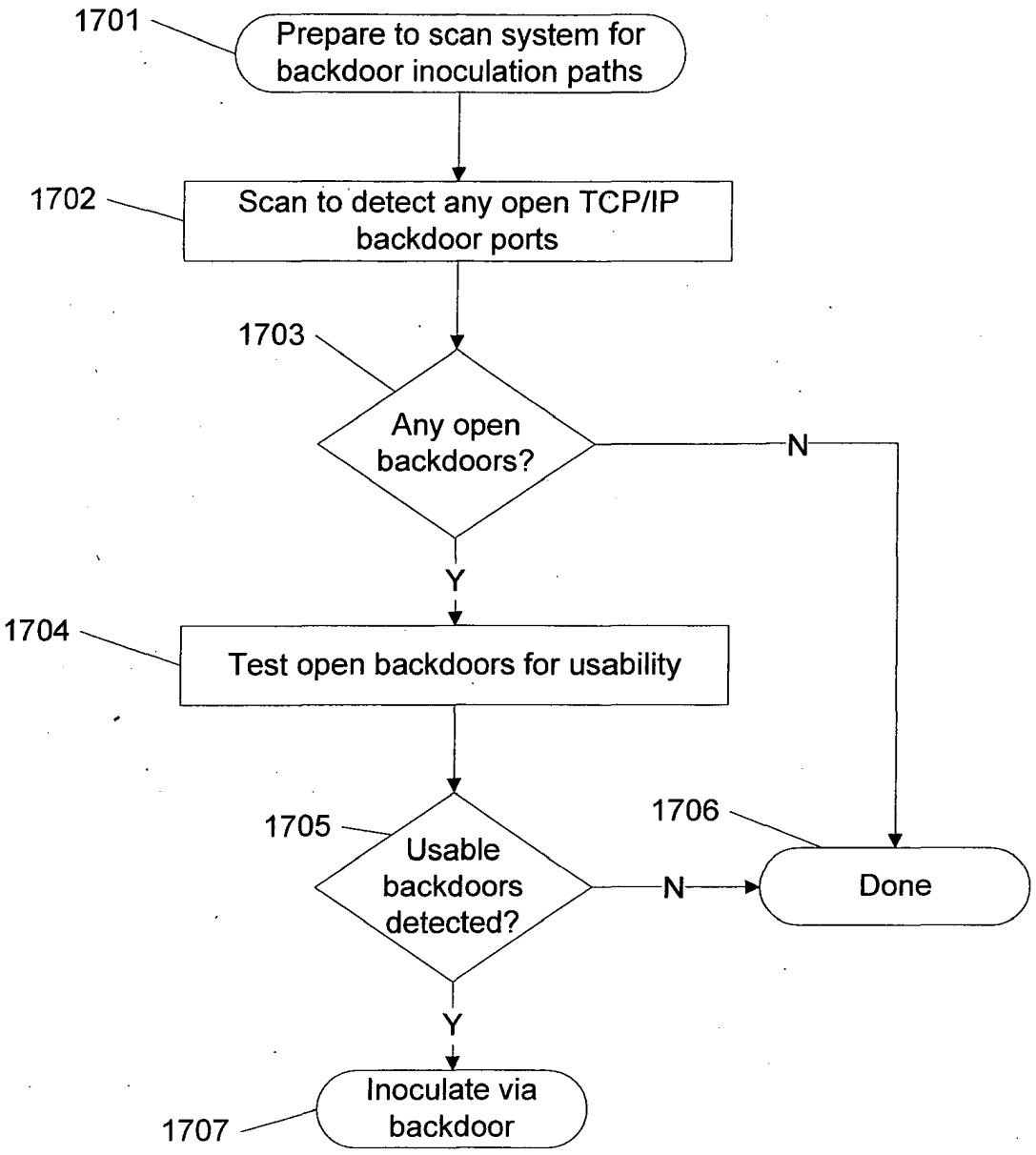

1701
Prepare to scan system for backdoor inoculation paths
1702
Scan to detect any open TCP/IP backdoor ports
1703
Any open backdoors?
N
Y
1704
Test open backdoors for usability
1705
Usable backdoors detected?
N
1706
Done
Y
Inoculate via backdoor
1707

Figure 17

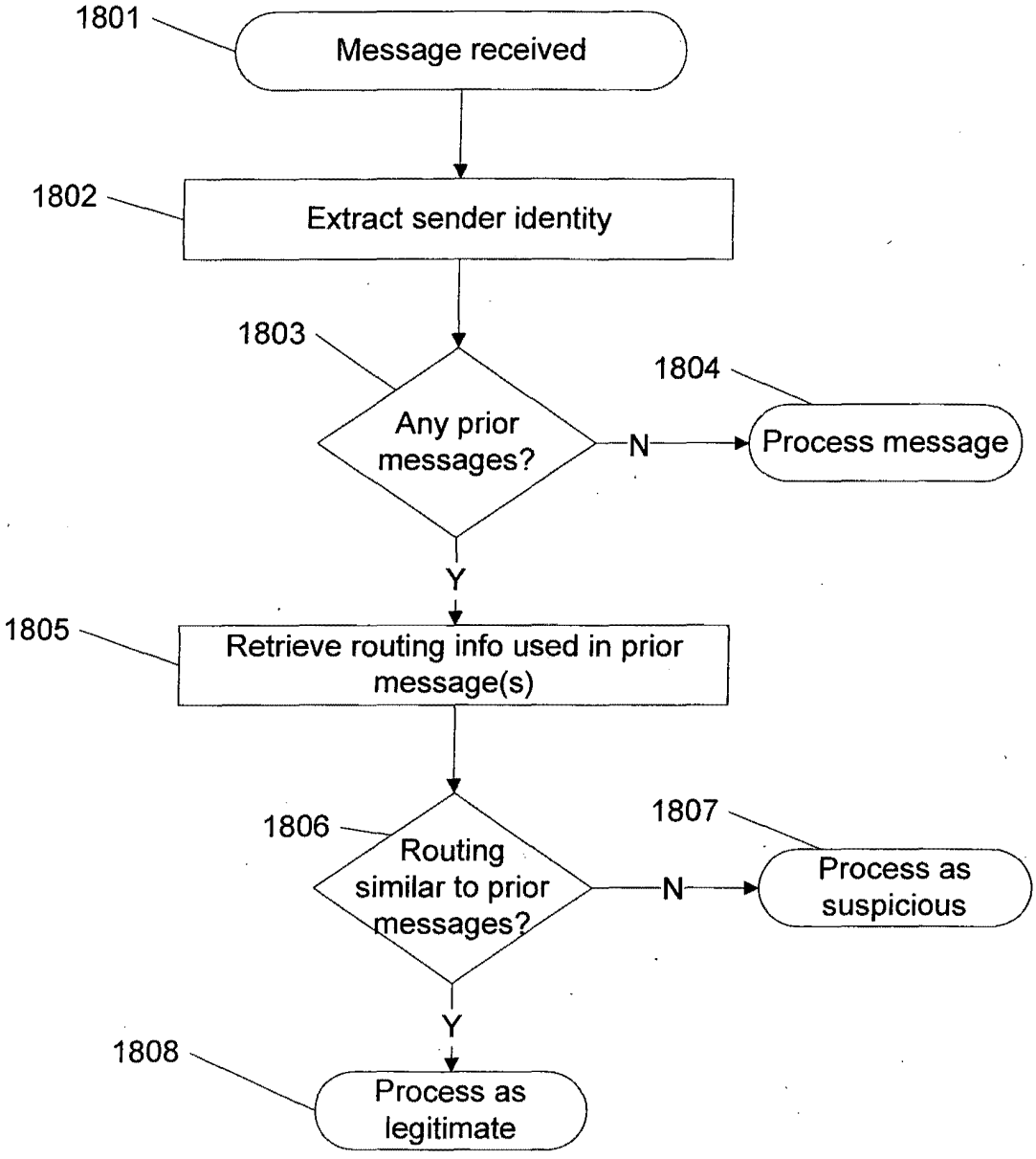

1801
Message received
1802
Extract sender identity
1803
Any prior messages?
N
1804
Process message
Y
1805
Retrieve routing info used in prior message(s)
1806
Routing similar to prior messages?
N
1807
Process as suspicious
Y
1808
Process as legitimate

Figure 18

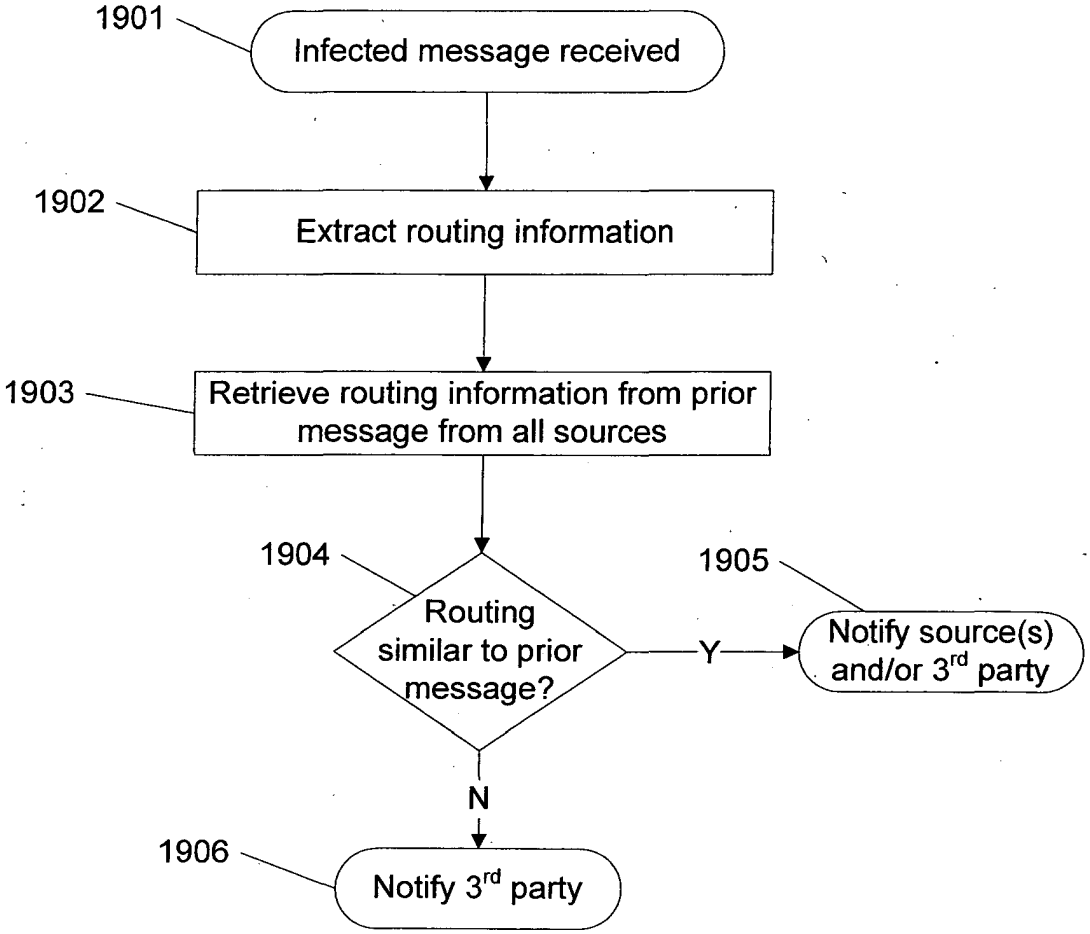

1901
Infected message received
1902
Extract routing information
1903
Retrieve routing information from prior message from all sources
1904
Routing similar to prior message?
Y
1905
Notify source(s) and/or 3rd party
N
1906
Notify 3rd party

Figure 19A

STAEDTLER® No. 937 811E
Engineer's Computation Pad

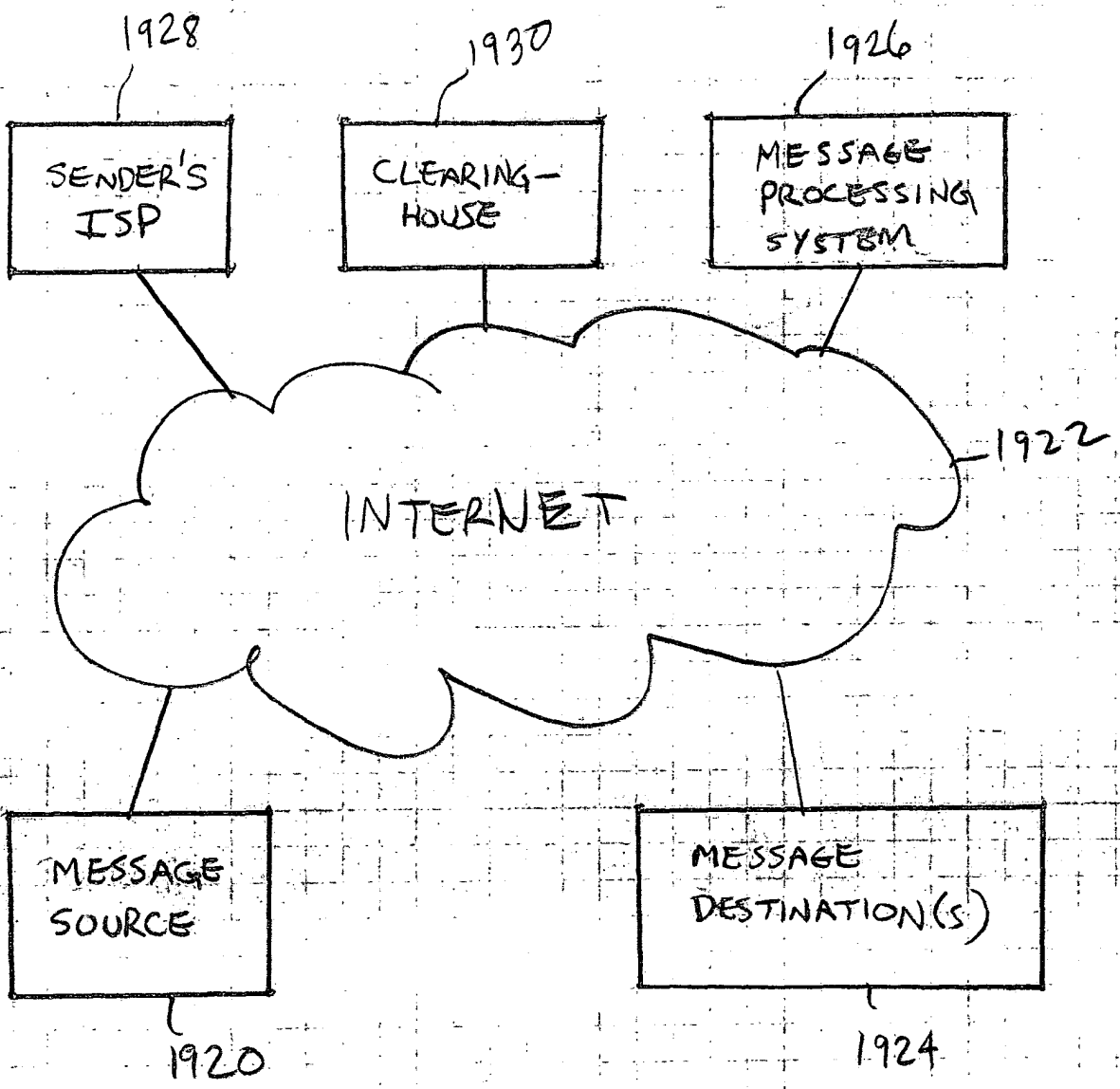


FIG. 19B

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. RAD2P003

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: DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS, 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	Jm A. Rosk			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. RAD2P003

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: DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS, 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)

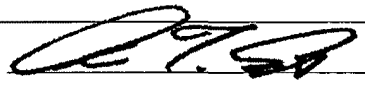
And I hereby appoint the law firm of Van Pelt, Yi & James LLP, including **Lee Van Pelt (Reg. No. 38,352); Susan C. Yi (Reg. No. 39,883); and William J. James (Reg. No. 40,661) Diana Y. Fu (Reg. No. 52,924) and Clover Huang (Reg. No. 55,285)** as my principal attorneys to prosecute this application and 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

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: 11237004

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	$200
TOTAL CLAIMS (37 CFR 1.16(i))	17 minus 20 =	—	X$ 25 =		OR	X$50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	1	X100 =	100		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	600		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.

PATENT APPLICATION SERIAL NO _____

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

09/30/2005 FFANAIA2 00000017 11237004

01 FC:2011	150.00	OP
02 FC:2111	250.00	OP
03 FC:2311	100.00	OP
04 FC:2201	100.00	OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 466-247/69033

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	DETECTING AND PROCESSING SUSPICIOUS NETWORK COMMUNICATIONS
	Attorney Docket Number	RAD2P003

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.