

communication connection; and enforce separation of the first communication connection from the second communication connection (Hatfalvi, Fig. 2, protected network, 220 SVM or special virtual machine; 240 Border Module and 250 Tunnel Restrictor Module; [0046] each protected computer comprises a special virtual machine (SVM) having a browser... communicates with the external network, such as the internet; [0048] lines 9-12, communications protocol...are modified so that all communications are tunneled and authenticated to the border module 240 for transmission to/from the external network; Examiner notes that the SVM would be accessing all websites which would include websites not in the whitelist).

11. As per **claim 33**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the host-based firewall is configured to prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system (Hatfalvi, [0028] The protected computer's 110 access to the protected network is limited to those communications specifically necessary for the remote operation... Other communications are generally prohibited. This isolation can be accomplished in hardware and/or software... damage to computers on the protected network is further prevented in the case of a compromised browser module).

12. As per **claim 34**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the device is configured to prevent unauthorized communication between the computer system and the one or more untrusted network destinations

(Hatfalvi, [0048] lines 9-12, communications protocol...are modified so that all communications are tunneled and authenticated to the border module 240 for transmission to/from the external network).

13. As per **claim 35**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the host-based firewall is configured to implement a first policy when the computer system is connected to the network and a second policy when the computer system is connected to another network, wherein the first policy permits one or more communications between the host system of the computer system and one or more resources on the network and the second policy blocks communications egressing from the host system of the computer system but allows communications egressing from the virtual system (Hatfalvi, Fig. 2, protected network, 220 SVM or special virtual machine; 240 Border Module and 250 Tunnel Restrictor Module; [0046] each protected computer comprises a special virtual machine (SVM) having a browser...communicates with the external network, such as the internet; [0048] normal network communications ability of the VM would traditionally allow an application direct local network and internet access... communications protocol...are modified so that all communications are tunneled and authenticated to the border module 240 for transmission to/from the external network; Examiner notes that the SVM would be accessing all websites which would include websites not in a whitelist policy while the host is restricted to access certain websites on another policy).

14. As per **claim 36**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein one or more applications or processes are configured to run in the virtual system, and wherein the one or more applications or processes running in the virtual system are configured to communicate with the one or more untrusted network destinations (Hatfalvi, Fig. 2, 240, 250; [0038] browser isolator module 130 and browser module 140...firewall; [0046] protected computer 210 comprises a special virtual machine (SVM) 220 having a browser 230... communicates with the external network 150; [0049] outbound traffic from the SVMs... forwarded to the external network 150).

15. As per **claim 37**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein one or more applications or processes are configured to run in the host system, and wherein the one or more applications or processes running in the host system are configured to communicate with one or more devices on the network (Hatfalvi, [0020] one or more protected computers 110... all connected by links 5; [0021] various components of these systems can be located at distant portions of a distributed network, such as a local area network, a wide area network, a telecommunications network, an intranet and/or the Internet).

16. As per **claim 38**, Hatfalvi discloses a method of network isolation in a networked computer system (Fig. 2, 200 Protected Network), the method comprising:

providing a network and at least one computer system that is configured to connect to the network (Fig. 1 and Fig. 2, external networks 150; [0026] external networks 150...provides its Internet-access services),

implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system ([0021] systems can be located at ... local area network, a wide area network, a telecommunications network, an intranet and/or the Internet or within a dedicated browser interface system or restricted tunneling system. ... components of these systems can be combined into one or more devices or collocated on a particular node of a distributed network, such as a protected network. ... the components of these systems can be arranged at any location within a distributed network without affecting the operation of the system; [0024] firewalls; [0025] protected network 100 includes a plurality of protected computers 110; [0028] The protected computer's 110 access to the protected network is limited to those communications specifically necessary for the remote operation... Other communications are generally prohibited. This isolation can be accomplished in hardware and/or software... damage to computers on the protected network is further prevented in the case of a compromised browser module);

providing at least one device configured to implement a network firewall or a web proxy ([0038] simple firewall; [0028] restricted router between the two; [0049]-[0050] border module 240... encapsulates and tunnels inbound external network communications to the end-user workstations SVMs... tunnel restrictor module 250); and

implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device (Fig. 2, 210 protected computer(s) all of which are located inside their respective Protected Networks 100 and 200).

Hatfalvi does not disclose the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system; separating the host system from the virtual system using an internal firewall executed on the computer system;

However, Reuben discloses the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system; separating the host system from the virtual system using an internal firewall executed on the computer system (1.

Introduction: multiple of these virtual machines can be run on a host computer, each processing its own operating system and application; 4.1 Communication between VMs or between VMs and host,... shared clipboard in virtual machine...allows data to be transferred between VMs and the host...; 4.2 VM Escape, This problem can be solved by properly configuring the host/guest interaction; 4.3 VM monitoring from the host, it is more necessary to strictly protect the host machines);

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to implement the teachings of Reuben because it would prevent the host's file system from becoming vulnerable in case the virtual machine is compromised.

17. As per **claims 39-47**, they are method claims of system claims 29-37, respectively. Therefore, they are rejected for the same reasoning as claims 29-37, above.

Conclusion

18. **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 WAYNE AN whose telephone number is (571)272-2028. The examiner can normally be reached on Monday - Friday 9-5 EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YIN-CHEN SHAW can be reached on (571)272-8593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number: 15/910,734
Art Unit: 2498

Page 14

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.

/WAYNE AN/
Examiner, Art Unit 2498

/THANHNGA B TRUONG/
Primary Examiner, Art Unit 2498

March 18, 2019

<i>Search Notes</i> 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner WAYNE AN	Art Unit 2498

CPC - Searched*		
Symbol	Date	Examiner
H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587	4/30/2018	WA
H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587	03/15/2019	WA

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor and assignee search	4/30/2018	WA
Limited text search using EAST and Google Scholar	4/30/2018	WA
Inventor and assignee search	03/15/2019	WA
Limited text search using EAST and Google Scholar	03/15/2019	WA

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/Wayne An/ Examiner, Art Unit 2498	
---------------------------------------	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	((("Hoy") near3 ("Robert") near3 ("B"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:08
S2	2	((("Fenkner") near3 ("Mark"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:19
S3	2	((("Farren") near3 ("Sean") near3 ("W"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:19
S4	24	("L3 Technologies").as.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:19
S5	20	("0000002" "0000017" "0000022" "0002010" "20020069369" "20060070066" "20070220187" "20070260873" "20080028401" "20080201711" "20080256536" "20090172781" "20090328038" "20100138829" "20100138830" "20100223613" "20100251329" "20120023593" "7478330" "7698442" "T000110").PN.	US-PGPUB; USPAT	OR	ON	2018/04/30 15:04
S6	25032	(H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587).cpc.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 15:04
S7	30248	(H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587).cpc.	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/14 23:11
S8	6323	(browser with (virtual adj2 machine))	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/14 23:11
S9	46	S8 and (permit\$4 permission restrict\$3 allow\$3) adj2 (communication transmission access\$3) with (predetermined (white adj list) whitelist)	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/14 23:12
S10	18	(isolat\$3 limit\$3 restrict\$3) adj (data adj transfer) same firewall	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/14 23:27
S11	0	(isolat\$3 limit\$3 restrict\$3) adj (data adj transfer) same firewall adj3 host	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/14 23:28

3/ 15/ 2019 6:43:02 PM

C:\Users\wan\Documents\EAST\Workspaces\15910734.wsp

DOCKET NO.: LCOM_ISO_US02
Application No.: 15/910,734
Office Action Dated: March 19, 2019

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
L3 Technologies, Inc.

Confirmation No.: 2365

Application No.: 15/910,734

Group Art Unit: 2498

Filing Date: March 2, 2018

Examiner: Truong, Thanhnga B.

For: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

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

Sir:

REPLY PURSUANT TO 37 CFR § 1.114

In response to the Official Action dated **March 19, 2019**, reconsideration is respectfully requested in view of the amendments and/or remarks as indicated below:

- ☐ **Amendments to the Specification** begin on page N/A of this paper.
- ☐ **Amendments to the Claims** are reflected in the listing of the claims which begins on page N/A of this paper.
- ☐ **Amendments to the Drawings** begin on page N/A of this paper and include an attached replacement sheet.
- ☒ **Remarks** begin on page 2 of this paper.
- ☒ The Commissioner is hereby authorized to charge any fee deficiency, charge any additional fees, or credit any overpayment of fees, associated with this application in connection with this filing, or any future filing, submitted to the U.S. Patent and Trademark Office during the pendency of this application, to Deposit Account No. 50-5519.

Electronic Acknowledgement Receipt

EFS ID:	36345764
Application Number:	15910734
International Application Number:	
Confirmation Number:	2365
Title of Invention:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS
First Named Inventor/Applicant Name:	Robert B. Hoy
Customer Number:	158266
Filer:	Ryan A. Peddle/melissa overline
Filer Authorized By:	Ryan A. Peddle
Attorney Docket Number:	LCOM_ISO_US02
Receipt Date:	19-JUN-2019
Filing Date:	02-MAR-2018
Time Stamp:	14:02:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 1300
RAM confirmation Number	061919INTEFSW14030400
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		LCOM_ISO_US02_AS_FILED_Response_to_Final_Office_Action_Dated_03_19_19.pdf	117854	yes	7
			bb8483e2658c566c32a24a6bdae9efd83a9e867		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Applicant Arguments/Remarks Made in an Amendment		2	7	
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	LCOM_ISO_US02_AS_FILED_RCE.pdf	79184	no	3
			525e116f02019d28e8a06de69c141c86ea6d6286		
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30409	no	2
			176d08c710296e3765ac0486db88ac3ed41c81		
Warnings:					
Information:					
Total Files Size (in bytes):			227447		

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.

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

Application Number	15910734	Filing Date	2018-03-02	Docket Number (if applicable)	LCOM_ISO_US02	Art Unit	2498
First Named Inventor	Robert B. Hoy			Examiner Name	Thanhnga B. Truong		

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

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

SUBMISSION REQUIRED UNDER 37 CFR 1.114

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

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

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

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

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 505519 _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (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 contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Ryan A. Peddle/	Date (YYYY-MM-DD)	2019-06-19
Name	Ryan A. Peddle	Registration Number	77970

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 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 the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

REMARKS

Claims 28-47 are pending in the application, of which claims 28 and 38 are independent. No claims have been amended. No claims have been added or cancelled. No new matter has been added.

In view of the following remarks, reconsideration of the pending rejections is respectfully requested.

Applicant Initiated Interview Summary

Applicant thanks Examiner Truong for participating in a telephonic interview with Applicant's undersigned representative on June 13, 2019. During the interview, the references cited in the Office Action and the pending claims were discussed. No formal agreement was reached.

Claim Rejections – 35 U.S.C. § 103

Claims 28-47 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over “Hatfalvi” (U.S. Patent Publication No. 2007/0260873) in view of NPL “Reuben” (“A survey on Virtual Machine Security”). Applicant respectfully requests reconsideration of the pending rejections in view of the following remarks.

Independent Claims 28 and 38

Independent claim 28 recites a networked computer system comprising...at least one computer system configured to connect to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system, ***wherein an internal firewall is configured to separate the host system from the virtual system in the computer system, and a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network; and at least one device configured to implement at least one of a network firewall or a web proxy, wherein the device comprises a processor***

and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system. Independent claim 38 recites similar subject matter. Simply stated, none of the asserted references, either alone or in combination, teach or suggest three distinct methods of isolation through a combination of an internal firewall, a host-based firewall, and a network firewall or web proxy as claimed.

For example, none of the references teach or suggest that ***a host-based firewall executed on the computer system*** is configured to ***implement network isolation between the computer system and the network***. Independent claim 38 similarly recites in part ***implementing network isolation between the computer system and the network*** using ***a host-based firewall executed on the computer system***. Such functionality for a host-based firewall executed on a computer system that is configured to implement network isolation between the computer system and the network is nowhere taught or suggested by either Hatfalvi or Reuben. For at least this reason, the rejections to claims 28 and 38 under 35 U.S.C. § 103 should be withdrawn.

Hatfalvi is completely silent with respect to ***a host-based firewall***. Hatfalvi generally discloses two main embodiments. The first, related to FIG. 1, utilizes a browser module 140 outside of a protected network 100 to perform browsing on behalf of one or more computers 110 utilizing a Browsing Client 120 within the protected network 100 (Hatfalvi, paras. [0020]-[0032]). In the second embodiment, related to FIG. 2, “[e]ach protected computer 210 comprises a special virtual machine (SVM) 220 having a browser 230. The browser 230 for each protected computer 210 communicates with the external network 150, such as the internet by means of a border module 240” (Hatfalvi, para. [0046]).

However, Hatfalvi nowhere teaches or suggests that either communications may be sent by the protected computer system that arise from applications outside of the SVM, or that some communications may be sent from the protected computer system to other resources on a local area network rather than to the Internet. Moreover, there is no mention in either embodiment of Hatfalvi that the protected computer systems include a host-based firewall, let alone that a host-based firewall executed on a protected computer system is configured to implement network isolation between the protected computer system and the protected network.

Thus, Hatfalvi cannot be said to teach or suggest that ***a host-based firewall executed on the computer system*** is configured to implement ***network isolation between the computer system and the network***, as recited in claim 28 and similarly in claim 38. Since Hatfalvi does not even teach or suggest the use of a host based firewall, it certainly cannot be said to teach or suggest a networked computer system comprising...at least one computer system configured to connect to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system, ***wherein an internal firewall is configured to separate the host system from the virtual system in the computer system***, and ***a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network***; and ***at least one device configured to implement at least one of a network firewall or a web proxy, wherein the device comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system***.

Reuben does not cure the deficiencies of Hatfalvi. For example, Reuben is also completely silent with respect to a host-based firewall. Instead, Reuben just generally discloses implementing one or more virtual machines (VMs) on a host machine (Reuben, Section 4.1). And, Reuben defines several security vulnerabilities associated with the virtual machines including communications between VMs, communications between VM(s) and host, VM escape, VM monitoring from host, VM monitoring from another VM, Denial of Service, Guest-to-Guest attack, external modification of a VM, and external modification of the hypervisor (Reuben, Sections 4.1-4.8). But, Reuben does not contemplate the VM being installed on a host machine that is located on a network with other devices, much less a host-based firewall executed on the host machine that is configured to implement network isolation between the host machine and the network. Further, like Hatfalvi Reuben nowhere contemplates how isolation can be achieved through a combination of an internal firewall, a host-based firewall, and a network firewall or web proxy.

Thus, Reuben does not correct the deficiencies of Hatfalvi. For example, Reuben, like Hatfalvi nowhere contemplates isolation of the host machine and virtual machines from a network on which the host machine is located. Rather, Reuben is wholly concerned with isolation of the virtual machines from each other on a single host system.

Thus, Reuben cannot be said to teach or suggest that ***a host-based firewall executed on the computer system*** is configured to implement ***network isolation between the computer system and the network***, as recited in claim 28 and similarly in claim 38. Moreover, Reuben cannot be said to teach or suggest a networked computer system comprising...at least one computer system configured to connect to the network, the computer system comprising a host system and a virtual system, wherein the virtual system is a separate operating system or a software module operating on the computer system, ***wherein an internal firewall is configured to separate the host system from the virtual system in the computer system***, and ***a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network***; and ***at least one device configured to implement at least one of a network firewall or a web proxy, wherein the device comprises a processor and a memory configured to implement network isolation between one or more untrusted network destinations and the networked computer system***.

As the asserted references fail to teach or suggest at least the above-referenced subject matter of independent claims 28 and 38. Accordingly, reconsideration and withdrawal of the rejection of claims 28 and 38 under 35 U.S.C. § 103 are respectfully requested.

Dependent Claims 33 and 43

Dependent claim 33 recites in part wherein ***the host-based firewall*** is configured to ***prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system***. Dependent claim 43 recites similar subject matter. As explained above, since neither Hatfalvi nor Reuben teach or suggest a host-based firewall at all, they also fail to teach or suggest these dependent claim features.

As discussed above, a local host-based firewall used on a computer system having a virtual system operating thereon is nowhere taught or suggested by Hatfalvi or Reuben. Further, neither Hatfalvi nor Reuben disclose a host-based firewall configured to prevent lateral communication and movement of malware between a computer system and other devices on a networked computer system.

And, as discussed above, the system of Hatfalvi nowhere teaches or suggests that some communications may be sent between resources on a local area network rather than simply with the Internet. Because Hatfalvi does not contemplate such communications between resources on a local area network, Hatfalvi also does not contemplate preventing movement of malware between a computer system and other devices on a networked computer system. Thus, Hatfalvi cannot be said to teach or suggest wherein *the host-based firewall* is configured to *prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system*, as recited in claim 33 and similarly in claim 43.

And as discussed above, Reuben does not contemplate the VM being installed on a host machine that is located on a network with other devices, much less *a host-based firewall* executed on the host machine that is configured to *prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system*. Thus, Reuben cannot be said to teach or suggest wherein *the host-based firewall* is configured to *prevent lateral communication and movement of malware between the computer system and other devices on the networked computer system*, as recited in claim 33 and similarly in claim 43.

As the asserted references fail to teach or suggest at least the above-referenced subject matter of dependent claims 33 and 43. Accordingly, reconsideration and withdrawal of the rejection of claims 33 and 43 under 35 U.S.C. § 103 are respectfully requested.

Dependent Claims 29-32, 34-37, 39-42, and 44-47

Insofar as dependent claims 29-32, 34-37, 39-42, and 44-47 depend either directly or indirectly from an allowable independent claim and further recite patentable subject matter,

DOCKET NO.: LCOM_ISO_US02
Application No.: 15/910,734
Office Action Dated: March 19, 2019

PATENT

Applicant respectfully submits that the dependent claims are also allowable over the asserted references. As such, Applicants request that the rejections to dependent claims 29-32, 34-37, 39-42, and 44-47 under 35 U.S.C. § 103 also be withdrawn.

CONCLUSION

The rejections set forth in the Office Action being adequately addressed, a Notice of Allowance is respectfully requested. Should Examiner Truong identify any outstanding issues that would prevent such an allowance, he is urged to contact Applicant's undersigned representative using the contact information contained below.

Date: June 19, 2019

Ryan A. Peddle/
Ryan A. Peddle
Registration No. 77,970

Condo Roccia Koptiw LLP
1800 JFK Blvd., Suite 1700
Philadelphia, PA 19103
Telephone: (215) 558-5740
Facsimile: (215) 558-5676

Electronic Patent Application Fee Transmittal

Application Number:	15910734			
Filing Date:	02-Mar-2018			
Title of Invention:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS			
First Named Inventor/Applicant Name:	Robert B. Hoy			
Filer:	Ryan A. Peddle/melissa overline			
Attorney Docket Number:	LCOM_ISO_US02			
Filed as Large 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- 1ST REQUEST	1801	1	1300	1300
Total in USD (\$)				1300

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/910,734	Filing Date 03/02/2018	☐ 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), (l), 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 \$ 100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		x \$ 460 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED - PART II

	(Column 1)		(Column 2)	(Column 3)	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	06/19/2019		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$ 100 = 0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0	x \$ 460 = 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			CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$ 0 =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$ 0 =
	☐ Application Size Fee (37 CFR 1.16(s))					
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
TOTAL ADD'L FEE						
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/SHERRY A DAVIS/
*** 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.

Notice of References Cited	Application/Control No. 15/910,734		Applicant(s)/Patent Under Reexamination Hoy et al.	
	Examiner THANHNGA B TRUONG		Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20060005188-A1	01-2006	Vega; Rene Antonio	G06F9/5077	718/1
*	B	US-20100251329-A1	09-2010	WEI; COACH	H04L63/1408	726/1
*	C	US-20100174811-A1	07-2010	Musiri; Sriram Srivathsan	G06F15/173	709/223
*	D	US-8185642-B1	05-2012	Tock; Theron	H04L63/102	709/225
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 2365

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
15/910,734	03/02/2018	726	2498	LCOM_ISO_US02		
RULE						
APPLICANTS L3 Technologies, Inc., New York, NY; INVENTORS Robert B. Hoy, Sewell, NJ; Mark Fenkner, Marlton, NJ; Sean W. Farren, Newburyport, MA; ** CONTINUING DATA ***** This application is a CON of 13/981,896 07/29/2013 PAT 9942198 which is a 371 of PCT/US2012/023027 01/27/2012 which claims benefit of 61/436,932 01/27/2011 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 03/28/2018						
Foreign Priority claimed ☐ Yes ☒ No	35 USC 119(a-d) conditions met ☐ Yes ☒ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Verified and /THANHNGA B	TRUONG/	Initials	NJ	2	20	2
Acknowledged	Examiner's Signature					
ADDRESS Condo Roccia Koptiw LLP 1800 JFK Boulevard Suite 1700 Philadelphia, PA 19103 UNITED STATES						
TITLE INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS						
FILING FEE RECEIVED 1880	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				



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.
15/910,734	03/02/2018	Robert B. Hoy	LCOM_ISO_US02	2365
158266	7590	07/25/2019	EXAMINER	
Condo Roccia Koptiw LLP 1800 JFK Boulevard Suite 1700 Philadelphia, PA 19103			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2498	
			MAIL DATE	DELIVERY MODE
			07/25/2019	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.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. 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 June 19, 2019. Claims 1-47 are pending. Claims 1-27 are cancelled by the applicant. At this time, claims 28-47 are rejected.

Notice of Pre-AIA or AIA Status

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

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 28-47 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 9, 942, 198 B2. Although the conflicting claims are not identical, they are not patentably distinct from each other because the two inventions have similar subject matter.

Allowable Subject Matter

3. Claims 28-47 would be allowable if a terminal disclaimer will be filed within the next amendment.

Conclusion

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

a. Vega; Rene Antonio et al (US 20060005188 A1) discloses Systems and methods for initializing multiple virtual processors within a single virtual machine (see Title).

b. WEI; COACH (US 20100251329 A1) discloses SYSTEM AND METHOD FOR ACCESS MANAGEMENT AND SECURITY PROTECTION FOR NETWORK ACCESSIBLE COMPUTER SERVICES (see Title).

c. Musiri; Sriram Srivathsan et al (US 20100174811 A1) discloses NETWORK ISOLATION AND IDENTITY MANAGEMENT OF CLONED VIRTUAL MACHINES (see Title).

d. Tock; Theron et al (US 8185642 B1) discloses Communication policy enforcement in a data network (see Title).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga B. Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Yin-Chen Shaw can be reached at 571-272-8593. The fax and

Application/Control Number: 15/910,734
Art Unit: 2498

Page 4

phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/THANHNGA B TRUONG/
Primary Examiner, Art Unit 2498

July 21, 2019

<i>Index of Claims</i> 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant					☐ CPA		☐ T.D.		☐ R.1.47	
CLAIM		DATE								
Final	Original	04/30/2018	03/15/2019	07/22/2019						
	1	-	-	-						
	2	-	-	-						
	3	-	-	-						
	4	-	-	-						
	5	-	-	-						
	6	-	-	-						
	7	-	-	-						
	8	-	-	-						
	9	-	-	-						
	10	-	-	-						
	11	-	-	-						
	12	-	-	-						
	13	-	-	-						
	14	-	-	-						
	15	-	-	-						
	16	-	-	-						
	17	-	-	-						
	18	-	-	-						
	19	-	-	-						
	20	-	-	-						
	21	-	-	-						
	22	-	-	-						
	23	-	-	-						
	24	-	-	-						
	25	-	-	-						
	26	-	-	-						
	27	-	-	-						
	28	✓	✓	✓						
	29	✓	✓	✓						
	30	✓	✓	✓						
	31	✓	✓	✓						
	32	✓	✓	✓						
	33	✓	✓	✓						
	34	✓	✓	✓						
	35	✓	✓	✓						
	36	✓	✓	✓						
	37	✓	✓	✓						
	38	✓	✓	✓						
	39	✓	✓	✓						
	40	✓	✓	✓						
	41	✓	✓	✓						
	42	✓	✓	✓						

<i>Index of Claims</i> 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

CLAIM		DATE								
Final	Original	04/30/2018	03/15/2019	07/22/2019						
	43	✓	✓	✓						
	44	✓	✓	✓						
	45	✓	✓	✓						
	46	✓	✓	✓						
	47	✓	✓	✓						

<i>Applicant-Initiated Interview Summary</i>	Application No. 15/910,734	Applicant(s) Hoy et al.	
	Examiner THANHNGA B TRUONG	Art Unit 2498	AIA (FITF) Status No

All participants (applicant, applicants representative, PTO personnel):

(1) THANHNGA B. TRUONG. (3) Mr. Joseph Klinicki.

(2) Mr. Ryan A. Peddle. (4) _____.

Date of Interview: 13 June 2019.

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: 28.

Identification of prior art discussed: See Continuation Sheet.

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's Representatives, Mr. Ryan A. Peddle and Mr. Joseph Klinicki, and Examiner discussed claimed invention. The application was reassigned to Examiner and more time needed to review and conduct a new search. Therefore, Mr. Peddle and Mr. Klinicki have decided that it was fair to file an RCE to give Examiner more time to work with the application. No agreement was reached..

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

	/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498
--	--

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 examiners 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 applicants 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 applicants 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 examiners 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 examiners initials.

Ex.1002

Continuation Sheet (PTOL-413)

Application No. 15/910,734

Continuation of Identification of prior art discussed: IDS - Hatfalvi (US2007/0260873) and Reuben ("A Survey on Virtual Machine Security")

Search Notes 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

CPC - Searched*		
Symbol	Date	Examiner
H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587	4/30/2018	WA
H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587	03/15/2019	WA
G06F9/46; G06F21/00; G06F15/173; H04L9/00; G06F21/53; G06F9/455 ; G06F15/16; H04L9/32; H04L63/0272; G06F9/45558; G06F21/53; H04L63/101	07/22/2019	TBT

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
718/726/709/713	718/1; 726/1,15; 709/223; 709/229; 709/235; 709/245; 726/24; 709/225; 713/170	07/22/2019	TBT

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor and assignee search	4/30/2018	WA
Limited text search using EAST and Google Scholar	4/30/2018	WA
Inventor and assignee search	03/15/2019	WA
Limited text search using EAST and Google Scholar	03/15/2019	WA
Inventor Name Searched; Assignee Searched	07/22/2019	TBT
TEXT Searched; EAST Searched; NPL Searched - Google/Patents and Scholar; STIC	07/22/2019	TBT

/Wayne An/ Examiner, Art Unit 2498	
---------------------------------------	--

<i>Search Notes</i> 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/Wayne An/ Examiner, Art Unit 2498	
---------------------------------------	--



computer system comprising a host system and a virtual system



Sign in

[All](#) [Images](#) [News](#) [Shopping](#) [More](#)
[Settings](#) [Tools](#)

About 1,080,000 results (0.41 seconds)

Virtual machine migration within a hybrid cloud system

www.google.com/patents/WO2017040326A1?ci=en


App - Filed Aug 26, 2016 - Published Mar 9, 2017 - Gabriel Tarasuk-Levin - VMware, Inc.
 ... workflow in the source virtualized computing system, where a host computer executing the ... computing system is a destination host in the second migration workflow. ... Rather, shadow VM 205 comprises software that mimics an actual VM.

[Overview](#) · [Related](#) · [Discuss](#)

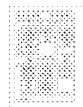
Virtual systems management

www.google.com/patents/US8799431


Grant - Filed Aug 10, 2008 - Issued Aug 5, 2014 - Vipul Pabari - Toutvirtual Inc.
 In network systems, with virtualization, it is possible to deploy physical ... Thus, the computer comprises a host machine for the virtualization environment. In FIG

[Overview](#) · [Related](#) · [Discuss](#)

Computer and method for directly accessing computer hardware by ...

www.google.com/patents/US20100125679


App - Filed Nov 20, 2009 - Published May 20, 2010 - Liang Tang - Lenovo (Beijing) Limited
 1, a virtual machine system typically comprises a virtual machine manager (e.g., ... and a method for directly accessing computer hardware by a virtual system, which ... comprises a PCI device and a BIOS used by the host operating system.

[Overview](#) · [Related](#) · [Discuss](#)

System and method for intelligent coordination of host and guest ...

www.google.com/patents/US20150012999


App - Filed Sep 22, 2014 - Published Jan 8, 2015 - William Gerald McGee - Trend Micro Incorporated

A distributed and coordinated security system providing intrusion-detection and intrusion-prevention for the virtual machines ... computer ... machine deployed on top of a virtualization platform of a virtual server system, comprising steps of

[Overview](#) · [Related](#) · [Discuss](#)

Managing message signaled interrupts in virtualized computer systems

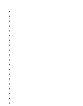
www.google.com/patents/US20160055108


App - Filed Aug 20, 2014 - Published Feb 25, 2016 - Alex Lee Williamson - Red Hat Israel, Ltd.

An example method may comprise, intercepting, by a hypervisor running on a host computer system, a memory read operation initiated by a virtual machine with ...

[Overview](#) · [Related](#) · [Discuss](#)

Virtual computer system and its i/o executive method

www.google.com/patents/CN85101171A?ci=en


App - Filed Apr 1, 1985 - Published Feb 11, 1987 - 梅野英典 - 株式会社日立製作所

A virtual computer system contained in a system can run simultaneously at least ... on the host system in the case where the VMCP directly without intervention, and ... CPU1006 FIG 7 comprises a pre-register 1010 (which includes prefix area

[Overview](#) · [Related](#) · [Discuss](#)

A computer system and method for controlling and/or monitoring a ...

www.google.com/patents/WO2011150929A1?ci=en


App - Filed May 27, 2011 - Published Dec 8, 2011 - Tage Kristensen - Vestas Wind Systems A/S

The wind power computer system (30) further comprises a hypervisor (40) ... as a host server, the hypervisor 40, and a plurality of virtual computer systems 54a- ...

[Overview](#) · [Related](#) · [Discuss](#)

Memory duplication by destination host in virtual machine live ...

www.google.com/patents/US9459902


Grant - Filed Aug 16, 2013 - Issued Oct 4, 2016 - Karen Noel - Red Hat Israel, Ltd.

An example method may comprise: receiving, by a hypervisor executing on a destination host computer system, a first virtual address and a corresponding ...

[Overview](#) · [Related](#) · [Discuss](#)

System and method to enhance memory protection for programs in a ...

www.google.com/patents/US8327056

Grant - Filed Sep 30, 2009 - Issued Dec 4, 2012 - Xiaoxin Chen - VMware, Inc.
in a computer system supporting execution of virtualization software and at least one instance of virtual system hardware, an interface is provided into the ... host ...
comprise ...
[Overview](#) · [Related](#) · [Discuss](#)

一种磁盘的访问方法及计算机系统 A disk access method and computer systems

www.google.com/patents/CN100375695B?cl=en

Grant - Filed Aug 23, 2010 - Issued Sep 23, 2015 - 李俊 - 联想(北京)有限公司
1 to FIG 1: prior art virtual machine system as an example, shows the ... [0053]
Preferably, the computer system further comprising a host operating
[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 [Next](#)

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

Virtual device context (VDC) integration for network services

S Sharma, NG Soni, R Desai, C Feng... - US Patent 9,178,912, 2015 - Google Patents
 ... 3 illustrates an example network 300 with an integrated VDC on a network switch 326 and extended to include a service node 302, according to one ... As noted, each service node 302, 304 may provide a variety of network management functions/services for traffic processed ...

☆ 55 Cited by 48 Related articles All 4 versions

A survey of intrusion detection techniques in cloud

C Modi, D Patel, B Borisaniya, H Patel, A Patel... - ... of network and computer ..., 2013 - Elsevier
 ... Mobile agent collects evidences of an attack from all the attacked VM for further analysis and auditing ... Moreover, a firewall GUI is used to configure firewall rules. Iptables application extension is used for authentication of rules configured by users and to parse the p.

☆ 55 Cited by 626 Related articles All 21 versions

Trusted compartmentalized computer operating system

PA McNabb, PS Slavin, CJ Hanson... - US Patent ..., 2001 - Google Patents
 ... For example, applications such as web browsers are typically configured to listen to a particular network interface to identify data destined for that application program where the program responds to and generates information that is directed through an Internet network ...

☆ 55 Cited by 350 Related articles All 2 versions

The eucalyptus open-source cloud-computing system

D Nurmi, R Wolski, C Grzegorzczak, G Obertelli... - ... Computing and the Grid, 2009 - dl.acm.org
 ... system is built to allow administra- tors and researchers the ability to deploy an infrastructure for user-controlled virtual machine creation and control atop existing resources ... We use a virtual networking solution that provides VM isolation, high performance, and a view of the ...

☆ 55 Cited by 2361 Related articles All 24 versions

System for allowing user of any computer to draw image over that generated by the host computer and replicating the drawn image to other computers

AA Carleton, CM FilzPatrick, TM Pommier... - US Patent ..., 1997 - Google Patents
 ... The two bitmaps are masked together. The annotation data is kept separate from the application data so that, for example, a user can save an Application image, but without annotations. Alternately, a user can save annotation data alone, or save an annotated display ...

☆ 55 Cited by 1422 Related articles All 2 versions

Operating system concepts

A Silberschatz, G Gagne, FB Galvin - 2018 - books.google.com
 ... Aside from explicit loads and stores, the CPU automatically loads instructions from main memory for execution from the location stored in ... A typical instruction-execution cycle, as executed on a system with a von Neumann architecture, first fetches an instruction from ...

☆ 55 Cited by 4450 Related articles All 55 versions

System and method for controlling interactions between networks

I Reid, S Minear - US Patent 6,182,226, 2001 - Google Patents
 ... This will cause ACL checks for transparent HTTP requests to bypass user nodes, and squid will ignore ... Since the proxy might not get an authentication filter after the ACLs return NEEDS_USERNAME, the squid proxy-auth code has been changed to not return a failure code ...

☆ 55 Cited by 469 Related articles All 2 versions

Firewall system for protecting network elements connected to a public network

CD Coley, RE Wesinger Jr - US Patent 5,826,014, 1998 - Google Patents
 ... of the user accessing the secure network 328, the identity of internal network elements is not revealed because the firewall 318, acting as an intermediary, shields the identity of the network elements for whom it is ... If an internal connection is tapped onto, a valid source ...

☆ 55 Cited by 413 Related articles All 2 versions

Secured session sequencing proxy system and method therefor

WJ Yarborough, JJ Zhuang - US Patent 6,718,388, 2004 - Google Patents
 ... Method for evolving detectors to detect malign behavior in an artificial immune system ... Accessing SSL connection data by a third-party. US8849716B1 (en), 2001-04-20, 2014-09-30, Jpmorgan Chase Bank, NA, System and method for preventing identity theft or misuse by ...

☆ 55 Cited by 79 Related articles All 2 versions

System for packet filtering of data packets at a computer network interface

GG Baehr, W Danielson, TL Lyon, G Mulligan... - US Patent ..., 1998 - Google Patents
... network(s) 335. For instance, a private network 335 may be an engineering domain
eng.sun.com in a company, while the private network 330 may be a corporate domain
corp.sun.com within the same company. The eng.sun ...

☆ ⓘ Cited by 235 Related articles All 2 versions ⓘ







All



Images



News



Videos



More

Settings

Tools

About 9,080 results (0.84 seconds)

Probabilistic Flow Management

www.google.com/patents/US20140366418


App - Filed Jun 5, 2013 - Published Dec 11, 2014 - Clinton Grant - Cisco Technology, Inc.
 If the number of **untrusted** flow objects exceeds the lower limit and prior to addition of the ...
 computer ... 1 is a block diagram of an example computing network having a **networking**
device configured to implement probabilistic flow ... with common packet parameters
 (source address, destination address, etc.) ...
[Overview](#) · [Related](#) · [Discuss](#)

Embedded security processor

www.google.com/patents/US5896499


Grant - Filed Feb 21, 1997 - Issued Apr 20, 1999 - Mark Ambrose McKelvey - International
 Business Machines Corporation
 The embedded security processor is controlled by the main processor and intercepts all
 communications from external **untrusted** or unverified network systems ...
[Overview](#) · [Related](#) · [Discuss](#)

Multi-level security network system

www.google.com/patents/US7069437


Grant - Filed Aug 22, 2001 - Issued Jun 27, 2006 - Timothy C. Williams - Cryptek, Inc.
 The security devices are interposed between each of workstation, including ... The result is
 trusted access to multiple secure Virtual Private Networks (VPN), ... use ... the evaluation of
 standalone computer systems, without networking, at a time ... Security Offices to
 configure and audit the operation of the secure network 10.
[Overview](#) · [Related](#) · [Discuss](#)

Networked facilities management system with optical coupling of ...

www.google.com/patents/US5550980


Grant - Filed Jan 7, 1994 - Issued Aug 27, 1996 - Gregory A. Pasucci - Johnson Service
 Company
 A networked system having a wide variety of applications and particularly applicable
 omitting such isolation exposes networks and sub-networks to complete ...
[Overview](#) · [Related](#) · [Discuss](#)

Method, apparatus and computer program product for a network firewall

www.google.com/patents/US7774836


Grant - Filed Aug 2, 2006 - Issued Aug 10, 2010 - Ken Xie - Juniper Networks, Inc.
 This improvement is provided without significant increase in the processing time ... A
 packet switch communication system includes a network of one or more routers ... A router
 is a switching device that receives packets containing data or control ... source, destination,
 port and protocol--to each rule in a rule set in sequence.
[Overview](#) · [Related](#) · [Discuss](#)

Communication policy enforcement in a data network

www.google.com/patents/US8185642


Grant - Filed Nov 18, 2005 - Issued May 22, 2012 - Theron Tock - Juniper Networks, Inc.
 The device is configured to provide at least one of the authorized data units ...
 communication between the device and the destination device. ... 1 is a diagram of an
 exemplary network 100 in which systems and ... untrusted ... that a computer-readable
 medium may include one or more memory ... isolation ...
[Overview](#) · [Related](#) · [Discuss](#)

Virtual network interface

www.google.com/patents/US8213429


Grant - Filed Aug 3, 2005 - Issued Jul 3, 2012 - Michael John Wray - Hewlett-Packard
 Development Company, L.P.
 This makes the virtual network more agile since changes to the virtual ... requires isolation of
 the network traffic, the data storage and processing of these ... the forwarding addresses to
 use for each packet, according to its destination ... systems, one of the problems is that
 current virtual machine technology does ... untrusted ...
[Overview](#) · [Related](#) · [Discuss](#)

Filters to isolate untrusted ports of switches

www.google.com/patents/US7305549


Grant - Filed May 25, 2004 - Issued Dec 4, 2007 - Galen C. Hunt - Microsoft Corporation



in one embodiment, a computing device having an un-configured SIPA is placed in ... of networks can be segregated into multiple VLANs for network isolation. ... Placing two or more computers in a VLAN is the equivalent of connecting ... memory ... the cryptographic processing engine of the SIPA 106 is implemented with ...
[Overview](#) · [Related](#) · [Discuss](#)

System for providing security in a network comprising communications ...

www.google.com/patents/US20080016332



App. - Filed Jul 11, 2007 - Published Jan 17, 2008 - James Holden - Micron Technology, Inc.
in one embodiment, the system is useful with an untrusted network, and comprises ... in network security is the use of computer devices in non-secure networks.
[Overview](#) · [Related](#) · [Discuss](#)

Method and system for enforcing security policies on network traffic

www.google.com/patents/US9059965



Grant - Filed Jun 30, 2009 - Issued Jun 16, 2015 - Nicolas G. Droux - Oracle America, Inc.
The computer readable medium causes the computer system to receive, by a data ... the invention relates to a computer system that includes a processor, a memory, ... in one or more embodiments of the invention, the data link rules are defined ... For example, if a packet source/destination is connected to a public network ...
[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 [Next](#)

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	21805	(G06F9/46; G06F21/00; G06F15/173; H04L9/00; G06F21/53; G06F9/455; G06F15/16; H04L9/32; H04L63/0272; G06F9/45558; G06F21/53; H04L63/101).cpc.	USPAT	OR	OFF	2019/07/22 08:23
L2	2456	l1 and ((computer with system) with ((host with system) and (virtual with system)))	USPAT	OR	OFF	2019/07/22 08:23
L3	1	l2 and ((internal with firewall) with ((configur\$3 with separat\$3) with ((host with system) and (virtual with system))))	USPAT	OR	OFF	2019/07/22 08:23
L4	0	l2 and (((host-based with firewall) with (execut\$3 with (computer with system))) with ((configur\$3 with implement\$3) with (network with isolation) with ((computer with system) with network)))	USPAT	OR	OFF	2019/07/22 08:24
L5	0	l2 and ((device with configur\$3) with (implement\$3 with ((network with firewall) or (web with proxy))))	USPAT	OR	OFF	2019/07/22 08:24
L6	0	l2 and (((device with configur\$3) with (implement\$3 with (network with isolation))) with ((untrust\$3 with network with destination) and (network\$3 with computer with system)))	USPAT	OR	OFF	2019/07/22 08:24
S162	5	"9942198".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/07/21 13:25
S163	70	("HOY, ROBERT" or "FENKNER, MARK" or "FARREN, SEAN").inv.	USPAT	OR	OFF	2019/07/22 06:47
S164	1	S163 and ((computer with system) with ((host with system) and (virtual with system)))	USPAT	OR	OFF	2019/07/22 06:48
S165	1	S163 and ((internal with firewall) with ((configur\$3 with separat\$3) with ((host with system) and (virtual with system))))	USPAT	OR	OFF	2019/07/22 06:50
S166	0	S163 and (((host-based with firewall) with (execut\$3 with (computer with system))) with ((configur\$3 with implement\$3) with (network with isolation) with ((computer with system) with network)))	USPAT	OR	OFF	2019/07/22 06:54
S167	0	S163 and ((device with configur\$3)	USPAT	OR	OFF	2019/07/22

		with (implement\$3 with ((network with firewall) or (web with proxy))))				06:55
S168	0	S163 and (((device with configur\$3) with (implement\$3 with (network with isolation))) with ((untrust\$3 with network with destination) and (network\$3 with computer with system)))	USPAT	OR	OFF	2019/07/22 06:58
S169	121	"L-3 COMMUNICATIONS CORP"	USPAT	OR	OFF	2019/07/22 06:59
S170	0	S169 and ((computer with system) with ((host with system) and (virtual with system)))	USPAT	OR	OFF	2019/07/22 06:59
S171	0	S169 and ((internal with firewall) with ((configur\$3 with separat\$3) with ((host with system) and (virtual with system))))	USPAT	OR	OFF	2019/07/22 06:59
S172	0	S169 and (((host-based with firewall) with (execut\$3 with (computer with system))) with ((configur\$3 with implement\$3) with (network with isolation) with ((computer with system) with network)))	USPAT	OR	OFF	2019/07/22 07:00
S173	0	S169 and ((device with configur\$3) with (implement\$3 with ((network with firewall) or (web with proxy))))	USPAT	OR	OFF	2019/07/22 07:00
S174	0	S169 and (((device with configur\$3) with (implement\$3 with (network with isolation))) with ((untrust\$3 with network with destination) and (network\$3 with computer with system)))	USPAT	OR	OFF	2019/07/22 07:00
S175	3	"20060005188".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/07/22 07:35
S176	2	"20100251329".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/07/22 07:42
S177	2	"20100174811".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/07/22 07:50
S178	3	"8185642".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/07/22 08:11
S179	95023	(718/1; 726/1,15; 709/223; 709/229; 709/235; 709/245; 726/24; 709/225; 713/170).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2019/07/22 08:16

			DERWENT; IBM_TDB			
S180	1093	S179 and ((computer with system) with ((host with system) and (virtual with system)))	USPAT	OR	OFF	2019/07/22 08:16
S181	0	S179 and ((internal with firewall) with ((configur\$3 with separat\$3) with ((host with system) and (virtual with system))))	USPAT	OR	OFF	2019/07/22 08:16
S182	0	S179 and (((host-based with firewall) with (execut\$3 with (computer with system))) with ((configur\$3 with implement\$3) with (network with isolation) with ((computer with system) with network)))	USPAT	OR	OFF	2019/07/22 08:16
S183	25	S179 and ((device with configur\$3) with (implement\$3 with ((network with firewall) or (web with proxy))))	USPAT	OR	OFF	2019/07/22 08:16
S184	0	S179 and (((device with configur\$3) with (implement\$3 with (network with isolation))) with ((untrust\$3 with network with destination) and (network\$3 with computer with system)))	USPAT	OR	OFF	2019/07/22 08:17

EAST Search History (Interference)

< This search history is empty >

7/ 22/ 2019 8:24:50 AM**C:\ Users\ ttruong4\ Documents\ EAST\ Workspaces\ Case-15910734-030218.wsp**



1. Embedded System

By: Tierney, Sade. Edition: 1st ed. Delhi : The English Press, 2011. eBook.
Description: Chapter 1- Introduction to Embedded System Chapter 2 -
Inertial Navigation System Chapter 3 - Motor Controller System Chapter 4 -
Anti-Lock Braking System Chapter 5 - Electronic Stability Control System
Chapter 6 - Cyber-Physical System & Anti-Hijack System Chapter 7 -
Digifant Engine Management System Chapter 8 - Real-Time Operating
System Chapter 9 - Immunity Aware Programming (AN 381852), Database:
eBook Collection (EBSCOhost)

Subjects: COMPUTERS / General; Embedded computer systems

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

2. Virtualization layer security challenges and intrusion detection/prevention **systems** in cloud computing: a comprehensive review.

By: Modi, Chirag; Acha, Kamatchi. *Journal of Supercomputing*. Mar2017. Vol. 73 Issue 3, p1192-1234. 43p. Abstract: Virtualization plays a vital role in the construction of cloud computing. However, various vulnerabilities are existing in current virtualization implementations, and thus there are various security challenges at virtualization layer. In this paper, we investigate different vulnerabilities and attacks at virtualization layer of cloud computing. We examine the proposals of cloud intrusion detection **system** (IDS) and intrusion detection and prevention **system** frameworks. We recommend the cloud IDS requirements and research scope to achieve desired level of security at virtualization layer of cloud computing. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s11227-016-1805-9. (AN: 121442516), Database: Academic Search Complete

Subjects: CLOUD computing; **VIRTUAL** machine **systems**; INTRUSION detection **systems** (Computer security); **FIREWALLS** (Computer security); **COMPUTER** network security; Data Processing, Hosting, and Related Services

PDF Full Text (2.5MB) USPTO Full Text Options

3. **System Center 2016 Virtual Machine Manager Cookbook, : Design, Configure, and Manage an Efficient Virtual Infrastructure with VMM in System Center 2016, 3rd Edition**

By: Levchenko, Roman; Cardoso, Edvaldo Alessandro. Edition: Third edition. Birmingham, UK : Packt Publishing. 2018. eBook. Description: Maximize your administration skills effectively and efficientlyKey FeaturesImplement cost-effective virtualization solutions for your organization with actionable recipesExplore the concepts of VMM with real-world use casesUse the latest features with VMM 2016 such as Cluster OS Rolling Upgrade, Guarded Fabric and Storage Spaces DirectBook DescriptionVirtual Machine Manager (VMM) 2016 is part of the System Center suite to configure and manage datacenters and offers a unified management experience ... (AN 1717559), Database: eBook Index

Subjects: **COMPUTERS** / System Administration / Windows Administration; **COMPUTERS** / System Administration / General; **COMPUTERS** / Cloud Computing; Cloud computing; Configuration management; **Virtual computer systems**



Full Text Finder

USPTO Full Text Options

4. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks.

By: Wang, Kai; Chen, Xi; Zhu, Yuefei. *PLoS ONE*. 5/10/2017, Vol. 12 Issue 5, p1-22. 22p. Abstract: Network address shuffling is a novel moving target defense (MTD) that invalidates the address information collected by the attacker by dynamically changing or remapping the host's network addresses. However, most network address shuffling methods are limited by the limited address space and rely on the host's static domain name to map to its dynamic address; therefore these methods cannot effectively defend against random scanning attacks, and cannot defend against an attacker who knows the target's domain name. In this paper, we propose a network defense method based on random domain name and address mutation (RDAM), which increases the scanning space of the attacker through a dynamic domain name method and reduces the probability that a host will be hit by an attacker scanning IP addresses using the domain name system (DNS) query list and the time window methods. Theoretical analysis and experimental results show that RDAM can defend against scanning attacks and worm propagation more effectively than general network address shuffling methods, while introducing an acceptable operational overhead. [ABSTRACT FROM AUTHOR] DOI: 10.1371/journal.pone.0177111. (AN: 122960233), Database: Academic Search Complete

Subjects: INTERNET domain naming **system**; **COMPUTER** operating **systems**; PHYSICAL sciences; APPLIED mathematics; **COMPUTER** simulation; Software Publishers; Software publishers (except video game publishers); Research and Development in the Physical, Engineering, and Life Sciences (except Biotechnology)

PDF Full Text (3.3MB) USPTO Full Text Options

5. Sustainable ICTs and Management Systems for Green Computing

By: Kaabouch, Naima; Hu, Wen Chen. Hershey, PA : IGI Global. 2012.
eBook. Description: "This book focuses on information technology using sustainable green computing to reduce energy and resources used"--
Provided by publisher. (AN 458135), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Electronics / Digital;
TECHNOLOGY & ENGINEERING / Electronics / Microelectronics; Electronic data processing departments; Electronic apparatus and appliances--
Environmental aspects; **Computer** networks--Energy conservation;
Telecommunication--Energy conservation; Green technology; Electronic data processing--Energy conservation

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

6. The role and security of **firewalls** in cyber-physical cloud computing.

By: Ullrich, Johanna; Cropper, Jordan; Frühwirth, Peter; Weippl, Edgar.
EURASIP Journal on Information Security, 8/12/2016, Vol. 2016 Issue 1, p1-20, 20p Abstract: Clouds are here to stay, and the same holds for cyber-physical **systems**-not to forget their combination. In light of these changing paradigms, it is of utter importance to reconsider security as both introduce new challenges. Overcoming the concept of zoned networks, clouds make former **internal** traffic traveling the Internet. Cyber-physical **systems** include physical parts into computing and make them potential targets for cyber attacks-a dare as a high number of physical parts have originally been developed to be stand-alone. Cyber-physical cloud computing reinforces the need for a thoughtful security concept. **Firewalls** are among the basic building blocks in network security and are offered by various cloud providers; however, the question on their quality of protection arises. In this paper, we assess **firewall** offers of five major cloud providers with respect to cyber-physical **system** integration. Therefore, we study their default configuration, configuration capabilities, documentation, and filtering behavior. We developed an extendible **firewall** monitoring tool that enables customers to probe their provider's filtering behavior-an information of interest for risk management or further security consideration. Re-assessing filtering behavior, we found that all offered **firewalls** have evolved over a time period of more than a year: Configuration possibilities have been enhanced, more illegitimate packets are filtered now, and stateful behavior was discovered at a certain provider. [ABSTRACT FROM AUTHOR]; DOI: 10.1186/s13635-016-0042-3; (AN 117380061), Database: Applied Science & Technology Source

Subjects: Computer security; **Firewalls** (Computer security); Cyber physical **systems**; Cloud computing; Internet service providers; All Other Telecommunications; Other telecommunications; Wired Telecommunications Carriers; Data Processing, Hosting, and Related Services

PDF Full Text (1.5MB) USPTO Full Text Options

7. A generic framework for application streaming service

By Malik, Asad W.; Rasool, Raihan ur; Anwar, Zahid; Nawaz, Shahid. In *Computers and Electrical Engineering*. February 2018 66:149-161
Language: English. DOI: 10.1016/j.compeleceng.2017.09.029 Abstract: The Cloud provides a shared computing environment to execute complex and compute intensive **virtual** appliances (VA). With network function virtualization and software defined networks, we are expected to see the physical network devices and their management consoles as VAs streamed on demand. Here, our focus is on the download mechanism that is used to distribute software that requires complex installation and rigid dependencies on the operating **system**. With limited bandwidth, it is difficult to download several pieces of software, especially with slow or sporadic internet connectivity. In this paper, we present a novel framework for application streaming named as Ceaseless Virtual Appliance Streaming (CVAS) **system** that offers **virtual** machine streaming through small executable blocks. The user can use a VA while it is being downloaded. The experimental section demonstrates the effectiveness of the proposed framework in terms of buffering time to execute **virtual** appliances. A feature analysis in comparison to competing approaches demonstrates that CVAS has improved buffering time, responsiveness and state pre-fetching accuracy. (AN: S0045790617309618), Database: ScienceDirect

Subjects: Streaming; Virtualization; **Virtual** machines; **Virtual** appliance; Cloud Computing



Full Text Finder

USPTO Full Text Options

8. Ports and Protocols Extended Control for Security.

By: Simpson, William R.; Foltz, Kevin E.. *IAENG International Journal of Computer Science*, May2017, Vol. 44 Issue 2, p72-85, 14p Abstract:
Network protocols have vulnerabilities, and one way to reduce these vulnerabilities is to reduce the protocols in use to a small set of well-tested standard protocols. This reduces the attack surface and provides high confidence in selected communications. Screening of acceptable ports and protocols can be done by network appliances known as **firewalls**. Communications on the approved list are permitted, and others blocked. Many appliances now have port and protocol filters, and the server or service itself may have a hostbased security **system** that can apply this functionality. This paper covers enterprise considerations for use and screening of ports and protocols. [ABSTRACT FROM AUTHOR]; (AN 123419636), Database: Applied Science & Technology Source

Subjects: Computer network protocols; Computer network security; Information technology security measures; **Firewalls (Computer security)**; Ports (Electronic **computer system**)

PDF Full Text (10.4MB) USPTO Full Text Options

9. **Handbook of Green Information and
Communication Systems**

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S.
Amsterdam : Academic Press. 2013. eBook. Description: This book gives a
comprehensive guide on the fundamental concepts, applications, algorithms,
protocols, new trends and challenges, and research results in the area of
Green Information and Communications **Systems**. It is an invaluable
resource giving knowledge on the core and specialized issues in the field,
making it highly suitable for both the new and experienced researcher in this
area. Key Features: Core research topics of green information and
communication **systems** are covered from a network ... (AN 485200),
Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing;
SCIENCE / Environmental Science; Sustainable engineering--Handbooks,
manuals, etc; Telecommunication--Environmental aspects--Handbooks,
manuals, etc; Telecommunication--Energy conservation--Handbooks,
manuals, etc

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

10. **Distributed Network Systems : From Concepts to Implementations**

By: Jia, Weijia; Zhou, Wanlei. Series: Network Theory and Applications, v. 15. New York : Springer. 2005. eBook. Description: This textbook covers both theoretical and practical aspects of distributed computing. It describes the client-server model for developing distributed network systems, the communication paradigms used in a distributed network system, and the principles of reliability and security in the design of distributed network systems. Based on theoretical introductions, the book presents various implementation strategies and techniques for building distributed network systems, including examples in TCP/IP communications, ... (AN 130165). Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Data Transmission **Systems** / General; **COMPUTERS** / Networking / Vendor Specific; **Computer** networks; Electronic data processing--Distributed processing

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

11. **Patent Issued for Multi-Node Virtual Data Storage Appliance With Internal Communications Filtering (USPTO 10,291,708)**

In: Information Technology Newsweekly. May 28, 2019, 4470; NewsRX LLC. Language: English. Abstract: 2019 MAY 28 (VerticalNews) -- By a News Reporter-Staff News Editor at Information Technology Newsweekly -- A patent by the inventors Lyon, Jared C. (Brighton, MA); De Smet, Jochen F. [...] (AN: edsgcl.586730013), Database: General OneFile

Subjects: Massachusetts; Data storage device; **Computer** storage devices -- Intellectual property

 [Full Text Finder](#) [USPTO Full Text Options](#)

12. Worm-Hunter: A worm guard **system** using software-defined networking

By: Hu, Yixun; Zheng, Kangfeng; Wang, Xu; Yang, Yixian. In: KSII Transactions on Internet and Information **Systems**. Jan 2017, Vol. 11 Issue 1, p484, 27 p.; KSII, the Korean Society for Internet Information Language: English. Abstract: Abstract Network security is rapidly developing, but so are attack methods. Network worms are one of the most widely used attack methods and have are able to propagate quickly. As [...] (AN: edsgcl487796795), Database: Academic OneFile

Subjects: Virus; **Virtual** private network; Data security issue; **Computer** viruses -- Control; **Virtual** private networks -- Methods; Data security -- Methods; Honeypots (Data security) -- Methods

Show all 23 images



PDF Full Text USPTO Full Text Options

13. Dynamic Construction Scheme for Virtualization Security Service in Software-Defined Networks.

By: Zhaowen Lin; Dan Tao; Zhenji Wang. *Sensors* (14248220). Apr2017, Vol. 17 Issue 4, p920. 18p. Abstract: For a Software Defined Network (SDN), security is an important factor affecting its large-scale deployment. The existing security solutions for SDN mainly focus on the controller itself, which has to handle all the security protection tasks by using the programmability of the network. This will undoubtedly involve a heavy burden for the controller. More devastatingly, once the controller itself is attacked, the entire network will be paralyzed. Motivated by this, this paper proposes a novel security protection architecture for SDN. We design a security service orchestration center in the control plane of SDN, and this center physically decouples from the SDN controller and constructs SDN security services. We adopt virtualization technology to construct a security meta-function library, and propose a dynamic security service composition construction algorithm based on web service composition technology. The rule-combining method is used to combine security meta-functions to construct security services which meet the requirements of users. Moreover, the RETE algorithm is introduced to improve the efficiency of the rule-combining method. We evaluate our solutions in a realistic scenario based on OpenStack. Substantial experimental results demonstrate the effectiveness of our solutions that contribute to achieve the effective security protection with a small burden of the SDN controller. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s17040920. (AN: 122915136), Database: Academic Search Complete

Subjects: SECURITY systems -- Management; VIRTUAL machine systems; COMPUTER software; ALGORITHMS; CONTROLLERSHIP; Computer and software stores; Computer, computer peripheral and pre-packaged software merchant wholesalers; Software publishers (except video game publishers); Computer and Computer Peripheral Equipment and Software Merchant Wholesalers; Security Systems Services (except Locksmiths)

PDF Full Text (2.4MB) USPTO Full Text Options

14. 'Configurable Internet Isolation And Security For Laptops And Similar Devices' in Patent Application Approval Process (USPTO 20190121961)

In: Information Technology Newsweekly. May 14, 2019, 1146; NewsRX LLC
Language: English. Abstract: 2019 MAY 14 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly -- A
patent application by the inventors Coleman, Glenn (Berwyn, PA); Martz,
Peter (Marlton, NJ); [...] (AN: edsgcl.585176527), Database: General OneFile

Subjects: United States; Telecommunications equipment industry; Internet
security; Laptop/portable **computer**; L3 Technologies, Inc. -- Intellectual
property; Telecommunications equipment industry -- Intellectual property;
Internet -- Safety and security measures; Laptop **computers**; Notebook
computers

 Full Text Finder USPTO Full Text Options

15. How to Implement Open-Source Solutions:
Firewalls.

By: Earley, Erwin. *System iNEWS*, Feb2012, Issue 388, following p24-24,
6p, 2 Color Photographs, 1 Black and White Photograph, 3 Diagrams
Abstract: In this article, the author focuses on the solutions offered by Linux,
a **computer operating system**, in order to improve security and stability of
computer systems. The author suggests that open-source **firewall** software
is more cost effective and it provides protection to information technology (IT)
infrastructure by preventing unauthorized access to the network. He further
informs that Linux **firewall** comes with a package called iptables to prevent
attacks from corrupted network packets.; (AN 72326012), Database: Applied
Science & Technology Source

Subjects: Linux operating **systems**; **Computer** access control; **Computer**
security; **Firewalls (Computer security)**; Data packeting

Show all 6 images



PDF Full Text (5.2MB) USPTO Full Text Options

16. A security and trust framework for virtualized networks and software-defined networking.

By: Yan, Zheng; Zhang, Peng; Vasilakos, Athanasios V.. *Security & Communication Networks*, 11/10/2016, Vol. 9 Issue 16, p3059-3069, 11p

Abstract: With the great success of the second-generation wireless telephone technology and the third-generation mobile telecommunications technology, and the fast development of the fourth-generation mobile telecommunications technology, the phase of fifth-generation mobile networks or fifth-generation wireless **systems** (5G) is coming. In this article, we indicate the open research issues of 5G security and trust in the context of virtualized networking and software-defined networking. We further propose a framework of security and trust focusing on solving 5G network security issues. The proposed framework applies adaptive trust evaluation and management technologies and sustainable trusted computing technologies to ensure computing platform trust and achieve software-defined network security. It adopts cloud computing to securely deploy various trustworthy security services over the virtualized networks. We analyze that the framework can support and satisfy all security requirements specified in standardization. We also suggest future research work according to the proposed framework and discuss the advantages of our framework in terms of practical deployment. Copyright © 2015 John Wiley & Sons, Ltd. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.1243; (AN 119057636). Database: Applied Science & Technology Source

Subjects: Virtual networks; Software-defined networking (**Computer network technology**); **Computer security**; Mobile communication **systems**; Wireless Telecommunications Carriers (except Satellite); Cordless telephones; 5G networks

PDF Full Text (278KB) USPTO Full Text Options

17. **Key Vulnerabilities of Industrial Automation and Control Systems and Recommendations to Prevent Cyber-Attacks.**

By: Calvo, I.; Etxeberria-Agiriano, I.; Ifigo, M. A.; González-Nalda, P..
International Journal of Online Engineering , 2016, Vol. 12 Issue 1, p9-16, 8p
Abstract: Until recently, Industrial Automation and Control **Systems** (IACS) were largely isolated from corporate **systems** by means of proprietary protocols, which facilitated their protection against cyber-attacks under the principle of security through obscurity. However, the widespread adoption of the new communication technologies, such as the Internet protocols and wireless communications has changed this scenario. In recent years there have been many evidences of cyberattacks to IACS that exploit their vulnerabilities. Unfortunately, these attacks have increased significantly during the last five years, and quite clearly only the tip of the iceberg comes to the public knowledge. The purpose of this article is twofold: (1) to raise awareness about the security vulnerabilities that most companies are facing at their IACS and (2) to propose a roadmap that seeks to guide designers and programmers in the new and complex world of industrial cyber-security. [ABSTRACT FROM AUTHOR]; DOI: 10.3991/ijoe.v12i1.4888; (AN 112350306), Database: Applied Science & Technology Source

Subjects: Automatic control **systems**; Cyberterrorism; **Computer** network protocols; Wireless communications; **Computer** security; Other printing; Wireless Telecommunications Carriers (except Satellite); Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing; Road maps

PDF Full Text (5.2MB) **USPTO Full Text Options**

18. Endpoint **firewall** for local security hardening in academic research environment.

By: Sobeslav, Vladimir; Balik, Ladislav; Hornig, Ondrej; Horalek, Josef; Krejcar, Ondrej. *Journal of Intelligent & Fuzzy Systems*. 2017, Vol. 32 Issue 2, p1475-1484. 10p. Abstract: This article presents a security **system** proposal, providing a low-level endpoint security and network activity monitoring. Its focus is to provide a necessary information for local administrators, who does not necessarily have the knowledge of networking infrastructure or access to it, according to the security policies of a parent organization. The proposed **system** is designed for academic research environments, where it serves as a tool for an extended security in protection of sensitive data used in research and development against the local and remote threats. The developed **system** was extended to contain central security point which acts as a server with IDS/IPS capability and enrich the whole functionality of distributed firewalling **system**. [ABSTRACT FROM AUTHOR] DOI: 10.3233/JIFS-169143. (AN: 121054431), Database: Academic Search Complete

Subjects: FIREWALLS (Computer security); COMPUTER network security; WEBSITE security measures; DATA protection; DATA security; RECORDS management; Other business support services; Internet Publishing and Broadcasting and Web Search Portals; Computer systems design and related services (except video game design and development); Other Computer Related Services

PDF Full Text (1.8MB) USPTO Full Text Options

19. A study on attack information collection using virtualization technology.

By: Yang, Hwan-Seok. *Multimedia Tools & Applications*, Oct2015, Vol. 74 Issue 20, p8791-8799, 9p Abstract: Internet is used in all sectors of society by rapid changes in computing technology and expanded internet prevalence. But due to opposite effect of this, malicious code and damage of hacking is growing rapidly and the technique is becoming various. Attacker's attack patterns and information should be collected in order to reduce the damage and cope more aggressively to attack. In this paper, we propose a **system** which build honeypot farm using created **virtual** machine dynamically by utilizing honeypot to collect attack information and virtualization technology. The created **virtual** machines are managed by VMSC and protocol-based intrusion detection **system** which shows stable performance in mass traffic to attacker's intrusion detection is applied. Measurement of attack attempt and attack detection rate was measured to confirm the performance of the proposed **system** in this paper and the result of good performance through experiment was confirmed. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11042-013-1487-8; (AN 109466507), Database: Applied Science & Technology Source

Subjects: Internet; **Computer** security; Intrusion detection **systems** (**Computer** security); **Computer** performance; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; Honeypots (Network security)

PDF Full Text (834KB) USPTO Full Text Options

20. Encyclopedia of **Virtual** Communities and Technologies

By: Dasgupta, Subhasish. Hershey, PA : IGI Global. 2006. eBook.

Description: 'This encyclopedia of **virtual** communities and technologies provides a much needed integrated overview of all the critical concepts, technologies and issues in the area of **virtual** communities'--Provided by publisher. (AN 136243), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Data Transmission **Systems** / General; **COMPUTERS** / Networking / Vendor Specific; Electronic villages (**Computer** networks)--Encyclopedias; Telecommunication--Encyclopedias; **Virtual** reality--Encyclopedias

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

21. A Delay-Based Countermeasure Against the
Discovery of Default Rules in Firewalls.

By: Sattar, K.; Salah, K.; Sqalli, M.; Rafiq, R.; Rizwan, M. *Arabian Journal for Science & Engineering (Springer Science & Business Media B.V.)*.

Feb2017, Vol. 42 Issue 2, p833-844. 12p. Abstract: Denial of service (DoS) attack is purely malicious and commonly used to overwhelm a network system making network resources unavailable to legitimate users. One such DoS attack is to target the firewall system of the enterprise, whereby the attacker sends a large number of malicious packets to the firewall making it unavailable for the legitimate users. To launch a smart and effective DoS attack, an attacker makes priori assumption about the order of the ruleset of the firewall. An effective firewall does not reveal its ruleset, policies, or information to the attacker. In this paper, we first present a process that can be used by an attacker to reconnoiter a firewall system at leisure to collect information about ruleset of a target firewall. The collected information can be used by the attacker to launch a slow-rate DoS attack against the firewall. We then propose a countermeasure technique 'Delay Induced Response (DIR)' which utilizes the underlying principle of moving target defense as a cyber maneuver technique. In DIR, the network frequently changes its properties visible to the attacker in order to confuse the attacker from discovering information about the firewall policy or its ruleset. The primary objective in DIR is to delude the attacker in his efforts in discovering the order of the firewall ruleset-specifically, the last matching rule (also known as the 'default rule') in a firewall. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s13369-016-2359-0. (AN: 121237447). Database: Academic Search Complete

Subjects: FIREWALLS (Computer security); MALICIOUS accusation; INFORMATION theory; DENIAL of service attacks; COMPUTER network security

[PDF Full Text \(1.5MB\)](#) [USPTO Full Text Options](#)

22. The Science DMZ: A network design pattern for data-intensive science.

By: Dart, Eli; Rotman, Lauren; Tiemey, Brian; Hester, Mary; Zurawski, Jason. *Scientific Programming*. 2014, Vol. 22 Issue 2, p173-185. 13p. Abstract: The ever-increasing scale of scientific data has become a significant challenge for researchers that rely on networks to interact with remote computing **systems** and transfer results to collaborators worldwide. Despite the availability of high-capacity connections, scientists struggle with inadequate cyberinfrastructure that cripples data transfer performance, and impedes scientific progress. The Science DMZ paradigm comprises a proven set of network design patterns that collectively address these problems for scientists. We explain the Science DMZ model, including network architecture, **system** configuration, cybersecurity, and performance tools, that creates an optimized network environment for science. We describe use cases from universities, supercomputing centers and research laboratories, highlighting the effectiveness of the Science DMZ model in diverse operational settings. In all, the Science DMZ model is a solid platform that supports any science workflow, and flexibly accommodates emerging network technologies. As a result, the Science DMZ vastly improves collaboration, accelerating scientific discovery. [ABSTRACT FROM AUTHOR] DOI: 10.1155/2014/701405. (AN: 96193780), Database: Academic Search Complete

Subjects: **COMPUTER** network architectures; **COMPUTER systems**; CYBERINFRASTRUCTURE; BIT rate; INTERNET security; WORKFLOW; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; **Computer systems** design and related services (except video game design and development); **Computer Systems** Design Services

Show all 8 images



PDF Full Text (508KB) USPTO Full Text Options

23. **Computer and Information Security Handbook**

By: Vacca, John R. Series: The Morgan Kaufmann Series in **Computer Security**. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network ... (AN 248986), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Networking / General; **COMPUTERS** / Security / General; **Computer networks**--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

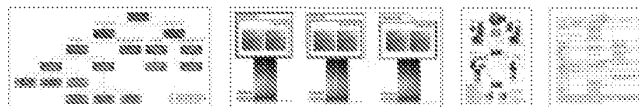
24. A Survey of Security Issues in Hardware Virtualization.

By: PÉK, GÁBOR; BUTTYÁN, LEVENTE; BENCSÁTH, BOLDIZSÁR. *ACM Computing Surveys*, Jun2013, Vol. 45 Issue 3, p40:1-40:34, 34p, 7

Diagrams, 2 Charts Abstract: Virtualization is a powerful technology for increasing the efficiency of computing services; however, besides its advantages, it also raises a number of security issues. In this article, we provide a thorough survey of those security issues in hardware virtualization. We focus on potential vulnerabilities and existing attacks on various virtualization platforms, but we also briefly sketch some possible countermeasures. To the best of our knowledge, this is the first survey of security issues in hardware virtualization with this level of details. Moreover, the adversary model and the structuring of the attack vectors are original contributions, never published before. [ABSTRACT FROM AUTHOR]; DOI: 10.1145/2480741.2480757; (AN 89005475), Database: Applied Science & Technology Source

Subjects: Computer input-output equipment; Computer security; Computer systems; Computing platforms; Vectors (Calculus); Computers; Computer Terminal and Other Computer Peripheral Equipment Manufacturing; Computer and peripheral equipment manufacturing; Computer, computer peripheral and pre-packaged software merchant wholesalers; Computer and Computer Peripheral Equipment and Software Merchant Wholesalers; Electronics Stores; Computer and software stores; Electronic Computer Manufacturing; Computer systems design and related services (except video game design and development); Computer Systems Design Services

Show all 9 images



PDF Full Text (611KB) USPTO Full Text Options

25. **Virtual LANs : A Guide to Construction, Operation, and Utilization**

By: Smith, Marina. Series: The McGraw-Hill Series on **Computer Communications**. New York : McGraw-Hill Professional. 1998. eBook. Description: Includes index. (AN 23083), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Networking / Local Area Networks (LANs); **COMPUTERS** / Data Transmission **Systems** / Broadband; **COMPUTERS** / Data Transmission **Systems** / Wireless; Local area networks (**Computer networks**)--**Computer programs**; **Virtual computer systems**

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

26. **Alan Simpson's Windows® XP Bible.**

By: Simpson, Alan. Series: Bible. Edition: 2nd ed. Indianapolis, IN : Wiley. 2005. eBook. Description: If Windows XP can do it, you can do it too... Windows XP is the undisputed market leader among operating systems, and the enhancements and security improvements in Service Pack 2 made it even better. So if you already know how to turn on a PC and use a mouse, here's the place to learn how to use every fabulous feature of Windows XP. Let an expert show you the new security features and help you customize your Windows, manage files, go online safely, work with digital media, set up a network, and solve ... (AN 127314), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Windows Desktop; Operating **systems (Computers)**

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

27. Hybrid file systems

By: International Business Machines Corporation. US Patent: 9,454,670.
Filed: December 03, 2012. Issued: September 27, 2016. , Database: USPTO
Patent Grants

Abstract: **Systems** and **computer** program products may provide a **virtual system** with direct access to one or more sectors of a resource of a **computer system**. The **system** and **computer** program products may include providing, by a **computer system** to a **virtual system**, first access control data associated with a regular **computer** file that corresponds to a resource on the **computer system**. The **system** and **computer** program products may additionally include receiving, at the **computer system**, a direct read from or direct write to one or more sectors of the resource represented by the regular **computer** file from the **virtual system**. The **system** and **computer** program products may further include hiding, at the **computer system**, a hidden **computer** file from the **virtual system**. The **system** and **computer** program products may additionally include routing, at the **computer system**, the direct read from or direct write to the hidden **computer** file on the **computer system**.

AN: edspgr.09454670

USPTO Full Text Options

28. Virtualization

By: Fukasawa, Naoto. In: Mobile Cloud Computing : Foundations and Service Models. 2018, p31-64. Language: English. Abstract: Virtualization . We have been lately hearing a lot about virtualization whenever there has been a talk about cloud computing. Although most of us may have ourselves used **virtual** machines [...] (AN: edsgcl.7437900012), Database: Gale Virtual Reference Library



Full Text Finder

USPTO Full Text Options

29. Essential **System** Administration

By: Frisch, AEleen. Series: A Nutshell Handbook. Edition: 2nd ed.
Sebastopol, CA : O'Reilly Media. 1995. eBook. (AN 24420). Database:
eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / **System** Administration / Linux & UNIX
Administration; Operating **systems** (**Computers**)

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

30. Hybrid file **systems**

By: International Business Machines Corporation. US Patent: 9,471,802.
Filed: October 28, 2013. Issued: October 18, 2016. , Database: USPTO
Patent Grants

Abstract: Methods may provide a **virtual system** with direct access to one or more sectors of a resource of a **computer system**. The method may include providing, by a **computer system** to a **virtual system**, first access control data associated with a regular **computer** file that corresponds to a resource on the **computer system**. The method may additionally include receiving, at the **computer system**, a direct read from or direct write to one or more sectors of the resource represented by the regular **computer** file from the **virtual system**. The method may further include hiding, at the **computer system**, a hidden **computer** file from the **virtual system**. The method may additionally include routing, at the **computer system**, the direct read from or direct write to the hidden **computer** file on the **computer system**.

AN: edspgr.09471802

[USPTO Full Text Options](#)

[EBSCO Support Site](#) | [Privacy Policy](#) | [Terms of Use](#) | [Copyright](#) | [Contact Us](#)

powered by EBSCOhost

© 2019 EBSCO Industries, Inc. All rights reserved.



1. NETWORK ISOLATION

Patent Application: 16/059381. Filed: August 09, 2018. Published: February 14, 2019. , Database: USPTO Patent Applications

Abstract: Methods and systems are disclosed for isolation of communications between a host computer system and one or more untrusted network destinations. An Internet isolation system may include a network, one or more host computer systems, a border firewall, an authorization device, and/or a proxy device. The Internet isolation system may be configured to implement network isolation between one or more untrusted network destinations, the one or more host computer systems, and/or the network. The network isolation may be implemented via one or more of a host-based firewall on each of the one or more host computer systems, the border firewall, the authorization device, the proxy device, an internal isolation firewall on each of the one or more host computer systems, and/or a segregation of a trusted memory space and an untrusted memory space on each of the one or more host computer systems.

AN: edspap.20190052604

USPTO Full Text Options

2. DATA EXFILTRATION SYSTEM AND METHODS

Patent Application: 16/144609. Filed: September 27, 2018. Published: March 28, 2019. . Database: USPTO Patent Applications

Abstract: A **host computer system** may be configured to connect to a **network**. The **host computer system** may be configured to implement a workspace and an isolated computing environment. The **host computer system** may be configured to isolate the isolated computing environment from the workspace using an internal **isolation firewall**. The internal **isolation firewall** may be configured to prevent data from being communicated **between** the isolated computing environment and the workspace, for example, without an explicit user input. When malware is received by the isolated computing environment, the internal **isolation firewall** may be configured to prevent the malware from accessing data on the workspace of the **host computer system**. The **host computer system** may be configured to implement one or more mechanisms that prevent malware received by the **host computer system** from exfiltrating, to a **network** destination, data from the **host computer system** and data from other devices on the **network**.

AN: edspap.20190097974

USPTO Full Text Options

3. SYSTEMS AND METHODS FOR COMMAND AND CONTROL PROTECTION

Patent Application: 16/146490. Filed: September 28, 2018. Published: March 28, 2019. , Database: USPTO Patent Applications

Abstract: A **host computer system** may be **configured** to connect to a **network**. The **host computer system** may be **configured** to implement a workspace and an isolated computing environment. The **host computer system** may be **configured** to isolate the isolated computing environment from the workspace using an internal **isolation firewall**. The internal **isolation firewall** may be **configured** to prevent data from being communicated **between** the isolated computing environment and the workspace, for example, without an explicit user input. The **host computer system** may be **configured** to implement one or more mechanisms that prevent malware received by the **host computer system** from receiving external communications from an external source. The one or more mechanisms may be **configured** to prevent control of the malware by the external source. The one or more mechanisms may be **configured** to prevent the malware from establishing a command channel with the external source.

AN: edspap.20190098020

USPTO Full Text Options

4. DOCUMENT ISOLATION

Patent Application: 16/138696. Filed: September 21, 2018. Published: March 28, 2019. , Database: USPTO Patent Applications

Abstract: Methods and **systems** are disclosed for document **isolation**. A **host computer system** may be **configured** to implement document **isolation** via one or more of a **host-based firewall**, an internet **isolation firewall**, and/or a segregation of a trusted memory space and an untrusted memory space. The **host computer system** may be **configured** to access one or more files using a first set of one or more applications and/or processes operating within the trusted memory space and/or a second set of one or more applications and/or processes operating within an untrusted memory space. The **host computer system** may be **configured** to open (e.g., always open) the one or more accessed files in the trusted memory space of the **host computer system**.

AN: edspap.20190097972

USPTO Full Text Options

5. HOST PROCESS AND MEMORY SEPARATION

Patent Application: 16/144761. Filed: September 27, 2018. Published: March 28, 2019. . Database: USPTO Patent Applications

Abstract: A **host computer system** may be configured to connect to a **network**. The **host computer system** may be configured to implement a workspace, an isolated computing environment, and a **host-based firewall**. The **host computer system** may be configured to isolate the isolated computing environment from the workspace using an **internal isolation firewall**. The **internal isolation firewall** may be configured to prevent data from being communicated **between** the isolated computing environment and the workspace, for example, without an explicit user input. The **host computer system** may be configured to determine, using one or more environmental indicators, a relative location of the **host computer system**. The processor may be configured to select a **firewall policy** based on the relative location of the **host computer system**. The **firewall policy** may include a configuration to apply to one or more of the **internal isolation firewall** or the **host-based firewall**.

AN: edspap.20190097975

USPTO Full Text Options

6. BROWSER SWITCHING SYSTEM AND METHODS

Patent Application: 16/146149. Filed: September 28, 2018. Published: March 28, 2019. , Database: USPTO Patent Applications

Abstract: A **host computer system** may be **configured** to connect to a **network**. The **host computer system** may be **configured** to implement a workspace and an isolated computing environment. The **host computer system** may be **configured** to isolate the isolated computing environment from the workspace using an internal **isolation firewall**. The **host computer system** may be **configured** to receive a request to communicate with a first **network** destination. On a condition that the first **network** destination is determined to be trusted, the processor may be **configured** to communicate with the first **network** destination via a first browser process **executed** in the workspace. On a condition that the first **network** destination is determined to be untrusted, the processor may be **configured** to communicate with the first **network** destination via a second browser process **executed** in the isolated computing environment.

AN: edspap.20190097977

USPTO Full Text Options

7. NETWORK ISOLATION FOR COLLABORATION SOFTWARE

Patent Application: 16/141535. Filed: September 25, 2018. Published: March 28, 2019. , Database: USPTO Patent Applications

Abstract: Methods and **systems** are disclosed for **isolation** of collaboration software on a **host computer system**. A networked computer system may include a **network**, a first **host computer system**, a border **firewall** and/or a web proxy. The **host computer system** may be **configured** to run a collaboration software application or process that enables interaction with one or more other **host computer systems**. The collaboration software application or process may be run within an untrusted memory space. The collaboration software application or process may enable interaction **between** a second **host computer system** and the untrusted memory space such that the second **host computer system** may access meeting data within a sandboxed computing environment operating within the untrusted memory space.

AN: edspap.20190097971

USPTO Full Text Options

8. **NETWORK ISOLATION WITH CLOUD NETWORKS**

Patent Application: 16/141378. Filed: September 25, 2018. Published: March 28, 2019. , Database: USPTO Patent Applications

Abstract: **Systems** and methods are disclosed for a sandbox **based network isolation system** configured to protect cloud based assets. A **host computer system** may include a processor and a memory. The **host computer system** may include a workspace. One or more applications may run in the workspace via a first memory space (e.g., a trusted memory space). The **host computer system** may include an isolated computing environment. One or more isolated applications may run in the isolated computing environment via a second memory space (e.g., an untrusted memory space). The isolated computing environment may be isolated from the workspace by an **internal isolation firewall**. The **internal isolation firewall** may prevent communication **between** the isolated computing environment and the workspace.

AN: edspap.20190097970

USPTO Full Text Options

9. **Researchers Submit Patent Application, 'Network Isolation', for Approval (USPTO 20190052604)**

In: Politics & Government Week. March 7, 2019, 15310; NewsRX LLC
Language: English. Abstract: 2019 MAR 7 (VerticalNews) -- By a News Reporter-Staff News Editor at Politics Government Week -- From Washington, D.C., VerticalNews journalists report that a patent application by the inventors Coleman, [...] (AN: edsgcl.576737255), Database: Academic OneFile



Full Text Finder

USPTO Full Text Options

10. CONFIGURABLE INTERNET ISOLATION AND SECURITY FOR MOBILE DEVICES

Patent Application: 16/163884. Filed: October 18, 2018. Published: April 25, 2019. , Database: USPTO Patent Applications

Abstract: **Systems**, methods, and instrumentalities are disclosed for providing configurable and customizable internet **isolation** and security schemes for a mobile device. A mobile device (e.g., a cell phone, smart phone, tablet, Internet of Things (IoT) device, etc.) may include a processor and a memory. The mobile device may be **configured to implement** a workspace and an isolated computing environment. The workspace may enable operation of a set of applications (e.g., trusted applications) via a memory space (e.g., a trusted memory space). The isolated computing environment may enable operation of a set of one or more applications (e.g., untrusted applications) via a memory space (e.g., an untrusted memory space). The untrusted applications may include, for example, one or more of an Internet browser, an email application, a document editing application, or a social media application. The untrusted applications may communicate with one or more untrusted **network** destinations via a **network**.

AN: edspap.20190121962

USPTO Full Text Options

11. 'Browser Switching **System** And Methods' in Patent Application Approval Process (USPTO 20190097977)

In: **Computer Weekly News**. April 17, 2019, 1320; NewsRX LLC Language: English. Abstract: 2019 APR 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Computer Weekly News** -- A patent application by the inventors Martz, Peter (Marlton, NJ); Moritz, Kenneth (Lansdowne, PA); [...] (AN: edsgcl.582284685), Database: General OneFile

Subjects: United States; Telecommunications equipment industry; Technology application; L3 Technologies, Inc. -- Intellectual property; L3 Technologies, Inc. -- Technology application; Telecommunications equipment industry -- Intellectual property; Telecommunications equipment industry -- Methods; Telecommunications equipment industry -- Technology application



Full Text Finder

USPTO Full Text Options

12. **Researchers Submit Patent Application, 'Sandbox Based Internet Isolation In An Untrusted Network', for Approval (USPTO 20190007257)**

In: Information Technology Newsweekly. Jan 22, 2019, 4599; NewsRX LLC
Language: English. Abstract: 2019 JAN 22 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly -- From
Washington, D.C., VerticalNews journalists report that a patent application by
the inventors Weinstein, [...] (AN: edsgcl.575451220), Database: General
OneFile

Subjects: United States; New York; Telecommunications equipment
industry; Internet; L3 Technologies, Inc. -- Intellectual property;
Telecommunications equipment industry -- Intellectual property



Full Text Finder

USPTO Full Text Options

13. **'Configurable Internet Isolation And Security For Laptops And Similar Devices' in Patent Application Approval Process (USPTO 20190121961)**

In: Information Technology Newsweekly. May 14, 2019, 1146; NewsRX LLC
Language: English. Abstract: 2019 MAY 14 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly -- A
patent application by the inventors Coleman, Glenn (Berwyn, PA); Maritz,
Peter (Marlton, NJ); [...] (AN: edsgcl.585176527), Database: General OneFile

Subjects: United States; Telecommunications equipment industry; Internet
security; Laptop/portable **computer**; L3 Technologies, Inc. -- Intellectual
property; Telecommunications equipment industry -- Intellectual property;
Internet -- Safety and security measures; Laptop **computers**; Notebook
computers



Full Text Finder

USPTO Full Text Options

14. **Method and system for network access control based on traffic monitoring and vulnerability detection using process related information**

By: Sophos Limited. US Patent: 10313,367. Filed: December 18, 2015.

Issued: June 04, 2019. , Database: USPTO Patent Grants

Abstract: Disclosed are various embodiments of method and **system** for **network** access control. The method may involve traffic monitoring and vulnerability detection using process information. The **system** may analyze the vulnerability as a process malfunctioning where preventive action focuses on process blocking as opposed to **host** blocking, which can lead to improved performance and productivity of a **network**. Techniques may use process related information, connection information, and **network** packet information for **network** control. The information may be matched against a plurality of signatures to identify and detect a known vulnerability in **network** activities. On the basis of a match, a verification report may be established. Techniques may further check whether a verification report is applicable to a process associated with a **network** packet and allow or block the process running on the **host based** in the report.

AN: edspgr.10313367

USPTO Full Text Options

15. **Computer and Information Security Handbook**

By: Vacca, John R. Series: The Morgan Kaufmann Series in **Computer Security**. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents information on how to analyze risks to your **networks** and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and **network** threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to **implement** security policies and procedures. In addition, this book covers security and **network** ... (AN 248986), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Networking / General; **COMPUTERS** / Security / General; **Computer networks--Security measures**

PDF Full Text **USPTO Full Text Options** **Download**

Table of Contents Most Relevant Pages From This eBook

16. Patent Application Titled 'Service Provider
Advanced Threat Protection' Published Online
(USPTO 20190068617)

In: Information Technology Newsweekly. March 19, 2019, 1900; NewsRX
LLC Language: English. Abstract: 2019 MAR 19 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly --
According to news reporting originating from Washington, D.C., by
VerticalNews journalists, a patent application [...] (AN: edsgcl.578807990),
Database: General OneFile

Subjects: United States; Telecommunications equipment industry; L3
Technologies, Inc. -- Intellectual property; Telecommunications equipment
industry -- Intellectual property



Full Text Finder

USPTO Full Text Options

17. A Survey on malware analysis and mitigation techniques

By Sibi Chakkaravarthy, S.; Sangeetha, D.; Vaidehi, V.. In *Computer Science Review*. May 2019 32:1-23 Language: English. DOI:

10.1016/j.cosrev.2019.01.002 Abstract: In recent days, malwares are advanced, sophisticatedly engineered to attack the target. Most of such advanced malwares are highly persistent and capable of escaping from the security systems. This paper explores such an advanced malware type called Advanced Persistent Threats (APTs). APTs pave the way for most of the Cyber espionages and sabotages. APTs are highly sophisticated, target specific and operate in a stealthy mode till the target is compromised. The intention of the APTs is to deploy target specific automated malwares in a host or network to initiate an on-demand attack based on continuous monitoring. Encrypted covert communication and advanced, sophisticated attack techniques make the identification of APTs more challenging. Conventional security systems like antivirus, anti-malware systems which depend on signatures and static analysis fail to identify these APTs. The Advanced Evasive Techniques (AET) used in APTs are capable of bypassing the stateful firewalls housed in the enterprise choke points at ease. Hence, this paper presents a detailed study on sophisticated attack and evasion techniques used by the contemporary malwares. Furthermore, existing malware analysis techniques, application hardening techniques and CPU assisted application security schemes are also discussed. Finally, the study concludes by presenting the System and Network Security Design (SNSD) using existing mitigation techniques. (AN: S1574013718301114), Database: ScienceDirect

Subjects: Evasion; Malware; Malware analysis; Packers; Sandboxes; Advanced persistent threats



Full Text Finder

USPTO Full Text Options

18. A holistic review of **Network Anomaly Detection Systems**: A comprehensive survey

By Moustafa, Nour; Hu, Jiankun; Slay, Jill. In *Journal of Network and Computer Applications*. 15 February 2019 128:33-55 Language: English. DOI: 10.1016/j.jnca.2018.12.006 Abstract: **Network Anomaly Detection Systems** (NADSs) are gaining a more important role in most **network defense systems** for detecting and preventing potential threats. The paper discusses various aspects of anomaly-based **Network Intrusion Detection Systems** (NIDSs). The paper explains cyber kill chain models and cyber-attacks that compromise **network systems**. Moreover, the paper describes various Decision Engine (DE) approaches, including new ensemble learning and deep learning approaches. The paper also provides more details about benchmark datasets for training and validating DE approaches. Most of NADSs' applications, such as Data Centers, Internet of Things (IoT), as well as Fog and Cloud Computing, are also discussed. Finally, we present several experimental explanations which we follow by revealing various promising research directions. (AN: S1084804518303886), Database: ScienceDirect

Subjects: Intrusion Detection **System** (IDS); **Network Anomaly Detection Systems** (NADS); Data pre-processing; Decision Engine (DE)



Full Text Finder

USPTO Full Text Options

19. Distribution and management of services in virtual environments

By: Microsoft Technology Licensing, LLC. US Patent: 10333,985. Filed: March 16, 2017. Issued: June 25, 2019. , Database: USPTO Patent Grants
Abstract: Distribution and management of services in virtual environments is described herein. In one or more implementations, a service distribution and management model is implemented in which **system** services and applications are seamlessly distributed across multiple containers which each **implement** a different runtime environment. In one or more implementations, a **system** for distributing access to services in a **host** operating **system** of a computing device includes a **host** operating **system** **configured to implement a host** runtime environment, and one or more services implemented by the **host** operating **system**. The **system** further includes a service control manager **configured** to enable communication **between** a client stub of a service implemented in a client runtime environment and a service provider of the service that is implemented in a service runtime environment that is separate from the first client runtime environment.

AN: edspgr.10333985

USPTO Full Text Options

20. Distribution and Management of Services in Virtual Environments

Patent Application: 16/277575. Filed: February 15, 2019. Published: June 13, 2019. , Database: USPTO Patent Applications

Abstract: Distribution and management of services in virtual environments is described herein. In one or more implementations, a service distribution and management model is implemented in which **system** services and applications are seamlessly distributed across multiple containers which each **implement** a different runtime environment. In one or more implementations, a **system** for distributing access to services in a **host** operating **system** of a computing device includes a **host** operating **system** configured to implement a **host** runtime environment, and one or more services implemented by the **host** operating **system**. The **system** further includes a service control manager configured to enable communication between a client stub of a service implemented in a client runtime environment and a service provider of the service that is implemented in a service runtime environment that is separate from the first client runtime environment.

AN: edspap.20190182295

USPTO Full Text Options

21. Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review

By Ullah, Faheem; Ali Babar, Muhammad. In *The Journal of Systems & Software*. May 2019 151:81-118 Language: English. DOI: 10.1016/j.jss.2019.01.051 Abstract: Highlights •SLR on architectural perspective of Big Data Cybersecurity Analytics (BDCA) **systems**.•Identification of 12 most widely emphasized quality attributes for BDCA **systems**.•Identification and codification of 17 architectural tactics for BDCA **systems**.•Identification of potential areas for future research in BDCA. (AN: S0164121219300172), Database: ScienceDirect

Subjects: Big data; Cybersecurity; Quality attribute; Architectural tactic



Full Text Finder

USPTO Full Text Options

22. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey

By Kumar, Rakesh; Goyal, Rinkaj. In *Computer Science Review*. August 2019 33:1-48 Language: English. DOI: 10.1016/j.cosrev.2019.05.002

Abstract: The world is witnessing a phenomenal growth in the cloud enabled services and is expected to grow further with the improved technological innovations. However, the associated security and privacy challenges inhibit its widespread adoption, and therefore require further exploration.

Researchers from academia, industry, and standards organizations have provided potential solutions to these challenges in the previously published studies. The narrative review presented in this survey, however, provides an integrationist end-to-end mapping of cloud security requirements, identified threats, known vulnerabilities, and recommended countermeasures, which seems to be not presented before at one place. Additionally, this study contributes towards identifying a unified taxonomy for security requirements, threats, vulnerabilities and countermeasures to carry out the proposed end-to-end mapping. Further, it highlights security challenges in other related areas like trust based security models, cloud-enabled applications of Big Data, Internet of Things (IoT), Software Defined Network (SDN) and Network Function Virtualization (NFV). (AN: S1574013718302065), Database: ScienceDirect

Subjects: Cloud computing; Security in cloud; Cloud security trust model; Cloud security challenges; Cloud security requirements threats vulnerabilities countermeasures



Full Text Finder

USPTO Full Text Options

23. A resource-preserving self-regulating Uncoupled MAC algorithm to be applied in incident detection

By Heigl, Michael; Doerr, Laurin; Tiefnig, Nicolas; Fiala, Dalibor; Schramm, Martin. In *Computers & Security*. January 2018 Language: English. DOI: 10.1016/j.cose.2019.05.010 Abstract: The connectivity of embedded systems is increasing accompanied with thriving technology such as Internet of Things/Everything (IoT/E), Connected Cars, Smart Cities, Industry 4.0, 5G or Software-Defined Everything. Apart from the benefits of these trends, the continuous networking offers hackers a broad spectrum of attack vectors. The identification of attacks or unknown behavior through Intrusion Detection Systems (IDS) has established itself as a conducive and mandatory mechanism apart from the protection by cryptographic schemes in a holistic security eco-system. In systems where resources are valuable goods and stand in contrast to the ever increasing amount of network traffic, sampling has become a useful utility in order to detect malicious activities on a manageable amount of data. In this work an algorithm – Uncoupled MAC – is presented which secures network communication through a cryptographic scheme by uncoupled Message Authentication Codes (MAC) but as a side effect also provides IDS functionality producing alarms based on the violation of Uncoupled MAC values. Through a novel self-regulation extension, the algorithm adapts it's sampling parameters based on the detection of malicious actions. The evaluation in a virtualized environment clearly shows that the detection rate increases over runtime for different attack scenarios. Those even cover scenarios in which intelligent attackers try to exploit the downsides of sampling. (AN: S0167404819301099), Database: ScienceDirect

Subjects: Network security; Adaptive intrusion detection; Message authentication; Self-regulation; Resource conservation



Full Text Finder

USPTO Full Text Options

24. Distribution and Management of Services in Virtual Environments

Patent Application: 15/460599. Filed: March 16, 2017. Published: July 12, 2018. , Database: USPTO Patent Applications

Abstract: Distribution and management of services in virtual environments is described herein. In one or more implementations, a service distribution and management model is implemented in which **system** services and applications are seamlessly distributed across multiple containers which each **implement** a different runtime environment. In one or more implementations, a **system** for distributing access to services in a **host** operating **system** of a computing device includes a **host** operating **system** configured to **implement** a **host** runtime environment, and one or more services implemented by the **host** operating **system**. The **system** further includes a service control manager configured to enable communication between a client stub of a service implemented in a client runtime environment and a service provider of the service that is implemented in a service runtime environment that is separate from the first client runtime environment.

AN: edspap.20180198824

USPTO Full Text Options

25. Network and System Security

By: Vacca, John R. Amsterdam : Syngress. 2014. eBook. Description: **Network and System** Security provides focused coverage of **network** and **system** security technologies. It explores practical solutions to a wide range of **network** and **systems** security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes building a secure organization, cryptography, **system** intrusion, UNIX and Linux security, Internet security, intranet security, LAN security; wireless ... (AN 596635), Database: eBook Index

Subjects: **COMPUTERS** / Security / General; **COMPUTERS** / **Systems** Architecture / General; **COMPUTERS** / Networking / General; **Computer networks**--Security measures



Full Text Finder

USPTO Full Text Options

26. Software defined cloud: Survey, **system** and evaluation

By Jararweh, Yaser; Al-Ayyoub, Mahmoud; Darabseh, Ala'; Benkhelifa, Elhadji; Vouk, Mladen; Rindos, Andy. In *Future Generation Computer Systems*. May 2016 58:56-74 Language: English. DOI: 10.1016/j.future.2015.10.015 Abstract: Next generation cloud **systems** will require a paradigm shift in how they are constructed and managed. Conventional control and management platforms are facing considerable challenges regarding flexibility, dependability and security that next generation **systems** must handle. The cloud computing technology has already contributed in alleviating a number of the problems associated with resource allocation, utilization and management. However, many of the elements of a well-designed cloud environment remain "stiff" and hard to modify and adapt in an integrated fashion. This includes the underlying networking topologies, many aspects of the user control over IaaS, PaaS or SaaS layers, construction of XaaS services, provenance and meta-data collection, to mention but few. In many situations the problem may be due to inadequacy of service abstraction. Software Defined **Systems** (SDSys) is a concept that help abstract the actual hardware at different layers with software components; one classical example of this abstractions are hypervisors. Such abstraction provides an opportunity for **system** administrators to construct and manage their **systems**, more easily, through flexible software layers. SDSys is an umbrella for different software defined subsystems including Software Defined Networking (SDN), Software Defined Storage (SDStorage), Software Defined Servers (Virtualization), Software Defined Data Centers (SDDC), Software Defined Security (SDSec) etc. and ultimately Software Defined Clouds (SDCloud). Individual solutions and seamless integration of these different abstractions remains in many respects a challenge. In this paper, the authors introduce Software Defined Cloud (SDCloud), a novel software defined cloud management framework that integrates different software defined cloud components to handle complexities associated with cloud computing **systems**. The first part of paper presents, for the first time, an extensive state of the art critical review of different components of software defined **systems**, constructing the proposed SDCloud. The second part of the paper proposes the novel concept of SDCloud, which is implemented and evaluated for its feasibility, flexibility and potential superiority. (AN: S0167739X15003283), Database: ScienceDirect

Subjects: Cloud computing; Software Defined **Systems**; Software Defined Security; Software Defined Storage; Software Defined Networking; Software Defined Cloud (SDCloud)



Full Text Finder

USPTO Full Text Options

27. Blockchain's adoption in IoT: The challenges, and a way forward

By Makhdoom, Imran; Abolhasan, Mehran; Abbas, Haider; Ni, Wei. In *Journal of Network and Computer Applications*. 1 January 2019 125:251-279
Language: English. DOI: 10.1016/j.jnca.2018.10.019 Abstract: The underlying technology of Bitcoin is blockchain, which was initially designed for financial value transfer only. Nonetheless, due to its decentralized architecture, fault tolerance and cryptographic security benefits such as pseudonymous identities, data integrity and authentication, researchers and security analysts around the world are focusing on the blockchain to resolve security and privacy issues of IoT. However, presently, not much work has been done to assess blockchain's viability for IoT and the associated challenges. Hence, to arrive at intelligible conclusions, this paper carries out a systematic study of the peculiarities of the IoT environment including its security and performance requirements and progression in blockchain technologies. We have identified the gaps by mapping the security and performance benefits inferred by the blockchain technologies and some of the blockchain-based IoT applications against the IoT requirements. We also discovered some practical issues involved in the integration of IoT devices with the blockchain. In the end, we propose a way forward to resolve some of the significant challenges to the blockchain's adoption in IoT. (AN: S1084804518303473), Database: ScienceDirect

Subjects: Blockchain; Internet of things; Consensus protocols; IoT security; Decentralized IoT; Blockchain challenges



Full Text Finder

USPTO Full Text Options

28. **MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach**

By Afzali Sereshti, Neda; Azmi, Reza. In *Engineering Applications of Artificial Intelligence*. October 2014 35:286-298 Language: English. DOI: 10.1016/j.engappai.2014.06.022 Abstract: This paper proposes an agent-based approach using artificial immune system (AIS) paradigms as a successful mechanism for a distributed intrusion detection system (IDS). The AIS paradigms are negative selection, clonal selection, danger theory, and immune network. These paradigms are very successful for anomaly IDS. The AIS paradigms are inspired by the powerful human immune system (HIS) and are promising candidate for design of an IDS. The proposed AIS-based agents are capable of learning, self-adaption, platform mobility, autonomy and collaboration. The proposed system (MAIS-IDS) was designed using these powerful and collaborative agents. This system has mobile and static agents with detector agents as the main actors in MAIS-IDS. The life cycles of agents are determined using the proposed immune algorithms in specific phases. Essential characteristics of MAIS-IDS are cloning, mutation, migration, collaboration, and randomness. MAIS-IDS was evaluated using a network of virtualized hosts, a kernel-based virtual machine (KVM) hypervisor and management Orchestra. (AN: S0952197614001444), Database: ScienceDirect

Subjects: Multi-agent; Intrusion detection system; Artificial immune system; Distributed system



Full Text Finder

USPTO Full Text Options

29. Telemetry analysis **system** for physical process anomaly detection

By: Accenture Global Solutions Limited. US Patent: 10148,686. Filed: February 10, 2017. Issued: December 04, 2018. , Database: USPTO Patent Grants

Abstract: **Systems**, methods, and apparatus, including **computer** programs encoded on **computer** storage media, for analyzing telemetry data from physical process sensors to detect anomalies within the physical process. A telemetry analytics **system** is disclosed as a process level anomaly detection **system based** on operational telemetrics and domain-specific knowledge that protects cyber physical **system** (CPS) devices against zero-day exploits not detectable through traditional **system** log or **network** packet inspection. The telemetry analytics **system** operates as a security component comparable to intrusion detection or anti-virus/anti-malware that generates alerts upon detecting anomalies in the sensor and/or activity data ingested from **system** or **network** data sources.

AN: edspgr.10148686

USPTO Full Text Options

30. A METHOD AND **SYSTEM** FOR **NETWORK**
ACCESS CONTROL **BASED** ON TRAFFIC
MONITORING AND VULNERABILITY
DETECTION USING PROCESS RELATED
INFORMATION

Patent Application: 15/527783. Filed: December 18, 2015. Published:
November 23, 2017. , Database: USPTO Patent Applications
Abstract: Disclosed are various embodiments of method and **system** for
network access control. The method may involve traffic monitoring and
vulnerability detection using process information. The **system** may analyze
the vulnerability as a process malfunctioning where preventive action focuses
on process blocking as opposed to **host** blocking, which can lead to
improved performance and productivity of a **network**. Techniques may use
process related information, connection information, and **network** packet
information for **network** control. The information may be matched against a
plurality of signatures to identify and detect a known vulnerability in **network**
activities. On the basis of a match, a verification report may be established.
Techniques may further check whether a verification report is applicable to a
process associated with a **network** packet and allow or block the process
running on the **host based** in the report.

AN: edspap.20170339172

USPTO Full Text Options

[EBSCO Support Site](#) | [Privacy Policy](#) | [Terms of Use](#) | [Copyright](#) | [Contact Us](#)

powered by EBSCOhost

© 2019 EBSCO Industries, Inc. All rights reserved.

A network perimeter with secure external access

FM Avolio, MJ Ranum, MD Glenwood - ... Symposium on Network and ... , 1994 - static.zedz.net
 ... Still, we believe that a **host-based firewall** is superior to other designs because of the ease ... initial connection to a general-purpose **network** listener inetd, which establishes a connection **between** ...
 For example, **an** incoming request for the TELNET service is "heard" by the **running** ...

☆ 57 Cited by 74 Related articles All 43 versions

Model based **systems** management in virtualized and non-virtualized environments

J Neystadt, Y Edery, Y Belinky, AB Vinberg - ... - US Patent ... , 2014 - Google Patents
 ... to validate and detect a discrepancy **between** the deployed service and **an** associated security ...
 according to a security model; deploying the virtual machine to a specific host ... locking down the
 virtual machine; and, **configuring firewall**, intrusion detection, and intrusion prevention ...

☆ 57 Cited by 57 Related articles All 4 versions

VL2: a scalable and flexible data center **network**

A Greenberg, JR Hamilton, N Jain, S Kandula - ... SIGCOMM computer ... , 2009 - dl.acm.org
 ... We analyzed hardware and software failures of switches, routers, load balancers, **firewalls**, links
 and servers using SNMP polling/traps, syslogs, server alarms, and transaction monitoring
 frameworks ... Hence, when **an** application sends a packet to **an** AA for the first time ...

☆ 57 Cited by 2367 Related articles All 68 versions

Virtual machine monitors: Current technology and future trends

M Rosenblum, T Garfinkel - Computer, 2005 - IEEE Explore.IEEE.org
 ... Current operating **systems** provide poor **isolation**, leaving **host-based** security mechanisms subject
 to attack ... Placing security outside a virtual machine pro- vides **an** attractive way to quarantine ... Virtual
 machines are also particularly well suited as a building block for constructing ...

☆ 57 Cited by 897 Related articles All 55 versions

Tamper-resistant, application-aware blocking of malicious **network** connections

A Srivastava, J Giffin - International Workshop on Recent Advances in ... , 2008 - Springer
 ... 2 Related Work Prior research has contributed to the development of conventional **host-based**
firewalls. Mogul et al ... without VMwall **running** inside dom0. All experiments were conducted on
 a machine with **an** Intel Core 2 Duo T7500 processor at 2.20 GHz with 2 GB RAM ...

☆ 57 Cited by 135 Related articles All 14 versions

... **system** including first program means translating user inputs into annotations and
running on all **computers** while second program means **runs** on one **computer**

KS Schwartz, AA Carleton, CM FitzPatrick - ... - US Patent ... , 1998 - Google Patents
 ... in a different way: The invention generates mouse messages at the **Host**, **based** on mouse ... any
 application program from a collection of application programs, which generates **an** image on ... **A**
system according to claim 1, wherein data from which the underlying image is derived ...

☆ 57 Cited by 1352 Related articles All 2 versions

Method and **system** for controlling access share storage devices in a **network**
 environment by **configuring** host-to-volume mapping data structures in the controller ...

WA Hubis, WG Delliz - US Patent 6,343,324, 2002 - Google Patents
 ... As the login procedure continues, controller 106 identifies a Host Index (HI) 151 for that **host based**
 on the ... in the table, and if it is present and the host has logged onto the array, only a check of ... For
 an array of N logical volumes, N Volume WWN Tables 130 (130-1, 130-2, 130-3 ...

☆ 57 Cited by 1050 Related articles All 2 versions

Principles of a **computer** immune **system**

A Somayaji, S Hofmeyr, S Forrest - NSPW, 1997 - people.scs.carleton.ca
 ... **Host-based** security can be thought of as the normal defenses a cell has against attack ... MIT Press.
 [13] BC Neuman and T. Ts'o. Kerberos: **An** authentica- tion service for **computer networks** ... [15]
 WA Wulf, C. Wang, and D. Kienzie. **A** new model of security for distributed **systems** ...

☆ 57 Cited by 473 Related articles All 30 versions

A survey of intrusion detection techniques in cloud

C Modi, D Patel, B Borisaniya, H Patel, A Patel... - ... of network and computer ..., 2013 - Elsevier

... Mobile agent collects evidences of **an** attack from all the attacked **VM** for further analysis and auditing ... IPSs are mainly classified into two categories: **Host based** IPS (HIPS) and **Network** based IPS (NIPS) ... Moreover, **a** **firewall** GUI is used to **configure** **firewall** rules ...

☆ 97 Cited by 626 Related articles All 21 versions

Network service for the detection, analysis and quarantine of malicious and unwanted files

J Oberheide, E Cooke, F Jahanian - US Patent 8,621,610, 2013 - Google Patents

... Briefly, the host agent 12 is **a** **host-based** software component that acquires files and forwards them to the ... The interface allows the querier to specify **a** broad range of filters including ... 4. **An** expression indicating what file names should be included in the query,; 5. The types of files ...

☆ 97 Cited by 265 Related articles All 4 versions




[Sign in](#)
[All](#) [Videos](#) [News](#) [Images](#) [More](#)
[Settings](#) [Tools](#)

About 67,300 results (0.46 seconds)

Method and system for testing internet software

www.google.com/patents/US7925692


Grant - Filed Jan 15, 2007 - Issued Apr 12, 2011 - Stephen Dunagan - Microsoft Corporation
The simulated internet has communications pathways between two **firewall devices**, a **web proxy** ... One or more test client machines on the corporate **network** are **configured to use** ... at least one additional vendor **web proxy**; and ... **least one additional vendor publishing firewall** to access said at least one test web server.
[Overview](#) · [Related](#) · [Discuss](#)

Secure network and method of establishing communication amongst ...

www.google.com/patents/US7024686


Grant - Filed May 11, 2001 - Issued Apr 4, 2006 - John Melvin Brawn - Hewlett-Packard Development Company, L.P.
Each anti bubble partition has at least one **network device configured to** ... Several types of **devices** have been developed that **perform network firewall** functions. ... Also, application proxies, e.g., socks and caching **web proxies**, allow specific ...
[Overview](#) · [Related](#) · [Discuss](#)

User authentication for proxy-configured clients in captive portal ...

www.google.com/patents/US9473495


Grant - Filed Sep 30, 2014 - Issued Oct 18, 2016 - Manish Manjunath Kadur - Avaya Inc.
The method can include, when received responses contain an IP address, replying ... **Network** ... to authenticate is client **device having proxy settings configured**. ... **portal** environments in accordance with at least one **implementation**. ... an **ignition server** made by Avaya Inc.), is **firewall 108**, the **Internet 110** ...
[Overview](#) · [Related](#) · [Discuss](#)

Method for implementing transparent gateway or proxy in a network

www.google.com/patents/US20080133774


App. - Filed Aug 14, 2007 - Published Jun 5, 2008 - Jai-hyoung Rhee - Rhee Jai-Hyoung
A **network device** applied to the above NAT stores an appropriate amount of ... at least one gateway or at least one **proxy**, by using a **network device** including a NAT table, ... If the destination port is set to as 80 and the **web proxy** is set to be the ... for address translation based on transparent **network** and **firewall web gate**.
[Overview](#) · [Related](#) · [Discuss](#)

Efficient transmission of IP data using multichannel SOCKS server proxy

www.google.com/patents/US20030177384

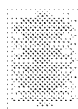

App. - Filed Mar 14, 2002 - Published Sep 18, 2003 - Douglas Jones - International Business Machines Corporation
Yet, the conventional SOCKS **proxy implementation** cannot provide is ... in the client computing device, and a split proxy server interface to at least one server ... The tunnel can host all Internet Protocol (IP) data traffic between the client ... 1 is a schematic illustration of a data communications **network configured with the split** ...
[Overview](#) · [Related](#) · [Discuss](#)

Systems and methods for remote access of network devices having ...

www.google.com/patents/US7975058


Grant - Filed Jan 31, 2006 - Issued Jul 5, 2011 - Anton Okmianski - Cisco Technology, Inc.
The proxy server is configured to retrieve the associated client device transport ... Voice Over Internet Protocol (VoIP) services, in particular, are gaining momentum, ... including those connected to a network behind a firewall, **Network Address** ... **devices** connected to a plurality of networks, where at least one **network** has ...
[Overview](#) · [Related](#) · [Discuss](#)

Transparent proxy of encrypted sessions

www.google.com/patents/US8504822


Grant - Filed Jul 3, 2012 - Issued Aug 6, 2013 - Jianxin Wang - Cisco Technology, Inc.
In one embodiment, a **proxy device** located between a first device and a ... from the first device that includes at least a subject name of the first device. ... Generally, **firewalls** are **devices** in computer networks that are **configured to apply one or** ... As more traffic within computer networks (e.g., the Internet) moves toward a ...
[Overview](#) · [Related](#) · [Discuss](#)

System and method for implementing a private virtual backbone on a ...

www.google.com/patents/US20060230431



App. - Filed Mar 31, 2005 - Published Oct 12, 2006 - Brian James - James Brian L.
The inter-bubble device and set of control points enforce the network security ... or internal web sites within the corporate network, inside the firewall, and the ... Additionally, the fact that a query may pass through one firewall device and a ... wherein said connecting device separates at least one local address space ...

[Overview](#) · [Related](#) · [Discuss](#)

Firewall proxy systems and methods in a backup environment

www.google.com/patents/US8572719



Grant - Filed May 27, 2011 - Issued Oct 29, 2013 - Andrei Erofeev - Commvault Systems, Inc.
Additionally, the method can include routing with the proxy device backup data from ... network firewalls to expose identification information, such as internet protocol ... The system comprises an enterprise network including at least one storage device, ... The proxy computing device may be configured to receive through the ...

[Overview](#) · [Related](#) · [Discuss](#)

Transparent web proxy

www.google.com/patents/US9002923



Grant - Filed Jul 1, 2008 - Issued Apr 7, 2015 - Junbiao Zhang - Thomson Licensing
When a party requests a web page, a TCP connection is set up between the ... The system can further include at least one proxy module in ... device use standard network protocols to discover a particular proxy ... firewall ...

[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 Next

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)





[All](#) [News](#) [Videos](#) [Images](#) [More](#)
[Settings](#) [Tools](#)

About 33,100 results (0.56 seconds)

System and method for providing network and computer firewall ...

www.google.com/patents/US9391956


Grant - Filed Jan 18, 2013 - Issued Jul 12, 2016 - Shlomo Touboul - Cupp Computing As
The computer may communicate with a firewall configured to handle both ... The network
address translation engine may be configured to use dynamic host ... diagram illustrating a
prior art network system having a software-based firewall ... netfilter, isolate user mobile
devices from the internet and run VPN program on the ...
[Overview](#) · [Related](#) · [Discuss](#)

System and method for protecting a computer system from malicious ...

www.google.com/patents/US7484247


Grant - Filed Aug 7, 2004 - Issued Jan 27, 2009 - Allen F Rozman - Allen F Rozman
The computer system is configured such that a malware program downloaded from the
network and executing on the second electronic data ... 20030097591, hosting computer
viruses ... correct level of isolation between programs ... Network firewalls are typically
based on packet filtering, which is limited in principle, since ...
[Overview](#) · [Related](#) · [Discuss](#)

Network firewall policy configuration facilitation

www.google.com/patents/US20040268150

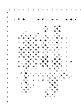

App. - Filed Jun 30, 2003 - Published Dec 30, 2004 - Jeffrey Aaron - Aaron Jeffrey A
Systems for providing information on network firewall policy configuration ... execution
system, apparatus, or device, such as a computer-based system ...
[Overview](#) · [Related](#) · [Discuss](#)

Network isolation techniques suitable for virus protection

www.google.com/patents/US20050050336


App. - Filed Oct 9, 2003 - Published Mar 3, 2005 - Yung Liang - Trend Micro Incorporated, A
Japanese Corporation
However, there exists a class of executable code that, if downloaded and executed at host
computers, may wreak havoc with the operating system, the hardware ...
[Overview](#) · [Related](#) · [Discuss](#)

Embedded security processor

www.google.com/patents/US5896499


Grant - Filed Feb 21, 1997 - Issued Apr 20, 1999 - Mark Ambrose McKelvey - International
Business Machines Corporation
Firewall systems must be initially set-up or configured, and occasionally must be ...
between computer systems and resources currently available via networks, ... based ...
Main processor 110 may be implemented as a single Central Processing ... executed by
embedded security processor 173 are protected, and cannot be ...
[Overview](#) · [Related](#) · [Discuss](#)

System and method for providing secure internetwork services via an ...

www.google.com/patents/US20040230791


App. - Filed May 26, 2004 - Published Nov 18, 2004 - William Boebert - Secure Computing
Corporation.
A system and method for the secure transfer of data between a workstation connected to ...
A secure computer is inserted into the private network to serve as the ...
[Overview](#) · [Related](#) · [Discuss](#)

System and method for protecting a computer system from malicious ...

www.google.com/patents/USRE43103


Grant - Filed Aug 10, 2010 - Issued Jan 10, 2012 - Allen F. Rozman - Rozman Allen F
The computer system is configured such that a malware program ... Network firewalls are
typically based on packet filtering, which is limited in principle, since ...
[Overview](#) · [Related](#) · [Discuss](#)

Process control methods and apparatus for intrusion detection, ...

www.google.com/patents/US7614083

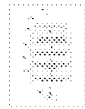

Grant - Filed Mar 11, 2005 - Issued Nov 3, 2009 - Bharat Khuti - Invensys Systems, Inc.
These networks utilize a combination of firewalls, intrusion detection systems, ... at
selected locations in and/or between the zones for (i) reporting network traffic, other host



digital data processors) that implement host-based intrusion protection. . The workstation 28, PC 30 and/or other digital data processing apparatus of ...
[Overview](#) · [Related](#) · [Discuss](#)

System and method for protecting a computer system from malicious ...

www.google.com/patents/USRE43987



Grant - Filed Jan 27, 2011 - Issued Feb 5, 2013 - Allen F. Rozman - Rozman Allen F
The computer system is configured such that a malware program ... Network firewalls are typically based on packet filtering, which is limited in principle, since ...
[Overview](#) · [Related](#) · [Discuss](#)

System and methods for providing network quarantine using IPsec

www.google.com/patents/US20060038580



App. - Filed Feb 14, 2005 - Published Apr 20, 2006 - Paul Mayfield - Microsoft Corporation
A system and method for ensuring that machines having invalid or corrupt states ... is directed to a computer network implementing a network isolation model.
[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 Next

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

Systems and methods for voluntary migration of a **virtual** machine between **hosts** with common storage connectivity

RA Vega, EP Traut, M Neil - US Patent 7,383,405, 2008 - Google Patents

... exemplary and other means of establishing a communications link between the **computers** may be ... machine," via a standard network connection between **computer hardware 102** and **computer hardware 102** ... With **host OS 104** initially having exclusive access to file **system 128** of ...

☆ ⓘ Cited by 248 Related articles All 4 versions ⓘ

Method and **system** for **virtual** port communications

IS Ganga - US Patent 8,798,056, 2014 - Google Patents

... G06F15/16—Combinations of two or more digital **computers** each having at least an arithmetic unit ... a laptop **computer**, a notebook **computer**, a terminal, a workstation, a server **computer**, a personal ... or may be implemented by, for example, VM **host** and edge switch **system 100** of ...

☆ ⓘ Cited by 383 Related articles All 4 versions ⓘ

Virtual **systems** management

V Pabari - US Patent 8,799,431, 2014 - Google Patents

Virtual systems management. Download PDF Info ... B2 US 8799431B2 Authority US United States Prior art keywords **virtual** virtualization **virtual** assets network ... Interpretation; Software simulation, eg virtualisation or emulation of application or operating **system** execution engines ...

☆ ⓘ Cited by 551 Related articles All 4 versions ⓘ

Apparatus and method for providing private and shared access to **host** address and data spaces by guest programs in a **virtual** machine **computer system**

DP Breisford, MM Cutler, JL Lafitte, JM Gdaniec... - US Patent ..., 1993 - Google Patents

... The interpretive-execution facility of Enterprise **Systems** Architecture/370(TM) (ESA/370(TM)) provides ... of the **virtual** machine guests; receiving a private-space signal from the **host computer system**; and ... selecting, from within a **host** access list comprising a plurality of entries, the ...

☆ ⓘ Cited by 166 Related articles All 2 versions ⓘ

Provisioning of **computer systems** using **virtual** machines

D Khandekar, D Petkovic, P Subrahmanyam... - US Patent ..., 2009 - Google Patents

... the provisioning server to monitor the operational state of the various **computers**, to maintain ... including the **hosts** within the overall provisioning **system** is that the **system** administrator can ... the user-selected "**computer**," no need to physically power on a **computer**, and, assuming ...

☆ ⓘ Cited by 511 Related articles All 3 versions ⓘ

Distributed **virtual** switch for virtualized **computer systems**

A Lambeth, S Zhou - US Patent 8,195,774, 2012 - Google Patents

... one of groups H04L1/00 - H04L27/00; H04L29/12—Arrangements, apparatus, circuits or **systems**, not covered ... for persisting a state of a **virtual** port in a virtualized **computer system** is described ... port (DVport) is stored in a persistent storage location, the DVport comprising a state ...

☆ ⓘ Cited by 437 Related articles All 4 versions ⓘ

System and method for **virtual** switching in a **host**

NG Droux, S Tripathi, E Nordmark - US Patent 7,643,482, 2010 - Google Patents

... 5, a networked **computer system** (200) includes a processor (202), associated memory (204), a ... 206), and numerous other elements and functionalities typical of today's **computers** (not shown). The networked **computer** (200) may also include input means, such as a keyboard ...

☆ ⓘ Cited by 215 Related articles All 4 versions ⓘ

Method, apparatus and **system** for improving security in a **virtual** machine **host**

EP Brickell, CD Hall, JF Cihula, RA Uhlig - US Patent 7,765,544, 2010 - Google Patents

... however, are often are used only after the virus has been detected and many **computers** have been ... These types of attacks can result in significant damage to the **computer system** ... US11/016,653 2004-12-17 2004-12-17 Method, apparatus and **system** for improving security in a ...

☆ ⓘ Cited by 174 Related articles All 4 versions ⓘ

Adjusting available persistent storage during execution in a **virtual computer system**

M Ginzton - US Patent 8,195,866, 2012 - Google Patents

... hand-held devices, microprocessor **systems**, microprocessor-based or programmable consumer electronics, minicomputers, mainframe **computers**, and the ... Everything in the **host system** 100 may be substantially the same as in existing **virtual computer systems**, except as ...

☆  Cited by 106 Related articles All 4 versions 

Method for establishing a **virtual** hard drive for an emulated **computer system** running on a **host computer system**

EP Traut, AS Giles, P Chakraborty - US Patent 6,968,350, 2005 - Google Patents

... that are unique to each client **computer** and are stored at the client **computers** or at ... in the differencing drive at client **computer systems** 502, allowing the client **computer systems** to access ... **comprising** the steps of: establishing in a hard drive of a **host computer system** a plurality ...

☆  Cited by 42 Related articles All 4 versions 

Internet isolation for avoiding internet security threats

RB Hoy, M Fenkner, SW Farren - US Patent 9,942,198, 2018 - Google Patents

A host computer supports a virtual guest system running thereon. The host system has a firewall that prevents it from communicating directly with the Internet, except with predetermined trusted sites. The virtual guest runs on a hypervisor, and the virtual guest comprises primarily a browser program that is allowed to contact the Internet freely via an Internet access connection that is completely separate from the host computer connection, such as a dedicated network termination point with its specific Internet IP address, or by ...

☆ ⓘ Related articles All 4 versions ⌕

Internet isolation for avoiding internet security threats

RB Hoy, M Fenkner, SW Farren - US Patent App. 15/910,734, 2018 - Google Patents

A host computer supports a virtual guest system running thereon. The host system has a firewall that prevents it from communicating directly with the Internet, except with predetermined trusted sites. The virtual guest runs on a hypervisor, and the virtual guest comprises primarily a browser program that is allowed to contact the Internet freely via an Internet access connection that is completely separate from the host computer connection, such as a dedicated network termination point with its specific Internet IP address, or by ...

☆ ⓘ All 2 versions ⌕

Showing the best results for this search. See all results

Xen and the art of virtualization

P Barham, B Dragovic, K Fraser, S Hand... - ... operating systems ..., 2003 - dl.acm.org
... means there **is** an additional protection domain **between** guest Oses and I/O **devices**, so it **is** ...
This structure **is** sufficiently generic to support a number of different **device** paradigms ... To aid validation, we associate a type and reference count with each **machine** page frame ...
☆ 57 Cited by 8640 Related articles All 189 versions

A survey of network virtualization

NMMK Chowdhury, R Boutaba - Computer Networks, 2010 - Elsevier
... The VPN states are stored in PE **devices**, and a connected CE **device** behaves as if it ... to allow service providers to simultaneously run **multiple** end-to-end services over **equipment** owned by ... Finally, with the increasing number of mobile and wireless **devices** and the onset of ...
☆ 57 Cited by 1312 Related articles All 17 versions

ClickOS and the art of network function virtualization

J Martins, M Ahmed, C Raiciu, V Oltanu... - ... on Networked Systems ..., 2014 - usenix.org
... leading tele- coms **network** operators, along with 52 other operators, IT and **equipment** vendors and ... 1, 42, 43], they typically lack driver support for a wide range of **devices** (especially NICs ... Conceptually, we would like to directly map ring packet buffers from the **device** driver or ...
☆ 57 Cited by 572 Related articles All 19 versions

Denali: Lightweight virtual machines for distributed and networked applications

A Whitaker, M Shaw, SD Gribble - 2002 - cs.ucsf.edu
... We **use** the OSKit as a hardware abstraction layer to simplify interactions with **devices**, page tables ... **use** Denali's interrupt and timer models, and linked the stack against a **device** driver for ... context switch time starts at 3.9 microseconds for a single virtual **machine**, and increases ...
☆ 57 Cited by 392 Related articles All 19 versions

The Click modular router

E Kohler, R Morris, B Chen, J Jannotti... - ... on Computer Systems ..., 2000 - dl.acm.org
... It also enables valuable configurations that are difficult to arrange otherwise—for example, a single queue feeding **multiple devices**, or a queue ... For example, it would be useful to refer to "the Ethernet address of the **device** handled by that FromDevice element ... Storage is a simple ...
☆ 57 Cited by 3009 Related articles All 55 versions

NetVM: High performance and flexible networking using virtualization on commodity platforms

J Hwang, KK Ramakrishnan... - ... Transactions on Network ..., 2015 - ieeeexplore.ieee.org
... in many cases, to fully exploit the agility benefits of virtual **machine**-based **network** ... 8: NetVM's architecture spans the guest and host systems; an emulated PCI **device** is used to ... The connection is implemented with a socket-type chardev with "-chardev socket,path=<path>,id=<id> ...
☆ 57 Cited by 328 Related articles All 17 versions

Systems and methods for transparent configuration authentication of networked devices

U Erlingsson, X Boyen, D Anderson, W Gray - US Patent 8,090,951, 2012 - Google Patents
... a bus 636 which couples **processor** 634 and **memory** 635, a mass storage **device** 637 (eg ... readable medium on the client and server systems, such as mass storage **devices** 627 and ... Examples of program instructions include **machine** code, such as produced by a compiler, and ...
☆ 57 Cited by 115 Related articles All 4 versions

System and method for securing networks

J Van De Groenendaal - US Patent 8,225,379, 2012 - Google Patents
... 1, wherein determining that the particular **one** of the identified authorized **devices** is bridging the first **network** and a second **network** comprises ... System and method for validating a location of an **untrusted device** ... System and method for migrating agents **between** mobile **devices** ...
☆ 57 Cited by 250 Related articles All 4 versions

Scale and performance in the Denali **isolation** kernel

A Whitaker, M Shaw, SD Gribble - ACM SIGOPS Operating Systems ..., 2002 - dl.acm.org

... emulation, **was implemented from scratch**; we used the Flux OS-Kit [14] for **device** drivers and ...

These virtual **devices** do not differ significantly from physical hardware **devices**, and we do not ...

case workload, the context switch time starts at 1.4 #s for a single virtual **machine**, and it ...

☆ 99 Cited by 563 Related articles All 47 versions

Network security **system** and method using a parallel finite state **machine** adaptive active monitor and responder

PC Hershey, DB Johnson, AV Le, SM Maiyas... - US Patent ..., 1995 - Google Patents

... I), and 202(E), to start three parallel, simultaneous, independently operating finite state **machine**

sequences shown in ... to **one of** the communicating **devices** 40 and 41 **or** to some other **device**

such as a ... paths may exist for the SA 10 to transmit responses to other **devices or** to take ...

☆ 99 Cited by 564 Related articles All 2 versions



1. NETWORK ISOLATION

Patent Application: 16/059381. Filed: August 09, 2018. Published: February 14, 2019. , Database: USPTO Patent Applications

Abstract: Methods and systems are disclosed for isolation of communications between a host computer system and one or more untrusted network destinations. An internet isolation system may include a network, one or more host computer systems, a border firewall, an authorization device, and/or a proxy device. The internet isolation system may be configured to implement network isolation between one or more untrusted network destinations, the one or more host computer systems, and/or the network. The network isolation may be implemented via one or more of a host-based firewall on each of the one or more host computer systems, the border firewall, the authorization device, the proxy device, an internal isolation firewall on each of the one or more host computer systems, and/or a segregation of a trusted memory space and an untrusted memory space on each of the one or more host computer systems.

AN: edspap.20190052604

USPTO Full Text Options

2. CONFIGURABLE INTERNET ISOLATION AND SECURITY FOR MOBILE DEVICES

Patent Application: 16/163884. Filed: October 18, 2018. Published: April 25, 2019. , Database: USPTO Patent Applications

Abstract: **Systems**, methods, and instrumentalities are disclosed for providing configurable and customizable internet **isolation** and security schemes for a mobile device. A mobile device (e.g., a cell phone, smart phone, tablet, Internet of Things (IoT) device, etc.) may include a **processor** and a **memory**. The mobile device may be **configured to implement** a workspace and an isolated computing environment. The workspace may enable operation of a set of applications (e.g., trusted applications) via a **memory space** (e.g., a trusted **memory space**). The isolated computing environment may enable operation of a set of **one or more** applications (e.g., **untrusted applications**) via a **memory space** (e.g., an **untrusted memory space**). The **untrusted** applications may include, for example, **one or more** of an Internet browser, an email application, a document editing application, or a social media application. The **untrusted** applications may communicate with **one or more untrusted network destinations** via a **network**.

AN: edspap.20190121962

USPTO Full Text Options

3. Blockchain Enabled Applications : Understand the Blockchain Ecosystem and How to Make It Work for You

By: Dhillon, Vikram; Melcalf, David; Hooper, Max. [New York, NY] : Apress. 2017. eBook. Description: Work with blockchain and understand its potential application beyond cryptocurrencies in the domains of healthcare, Internet of Things, finance, decentralized organizations, and open science. Featuring case studies and practical insights generated from a start-up spun off from the author's own lab, this book covers a unique mix of topics not found in others and offers insight into how to overcome real hurdles that arise as the market and consumers grow accustomed to blockchain based start-ups. You'll ... (AN 1641968), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Programming / Open Source; **COMPUTERS** / Human-**Computer** Interaction (HCI); Blockchains (Databases)

PDF Full Text USPTO Full Text Options Download

Table of Contents Most Relevant Pages From This eBook

4. **Computer and Information Security Handbook**

By: Vacca, John R. Series: The Morgan Kaufmann Series in **Computer Security**. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents information on how to analyze risks to your **networks** and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and **network** threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to **implement** security policies and procedures. In addition, this book covers security and **network** ... (AN 248988), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Networking / General; **COMPUTERS** / Security / General; **Computer networks**--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

5. **Distributed Network Systems : From Concepts to Implementations**

By: Jia, Weijia; Zhou, Wanlei. Series: **Network Theory and Applications**, v. 15. New York : Springer. 2005. eBook. Description: This textbook covers both theoretical and practical aspects of distributed computing. It describes the client-server model for developing distributed **network systems**, the communication paradigms used in a distributed **network system**, and the principles of reliability and security in the design of distributed **network systems**. Based on theoretical introductions, the book presents various implementation strategies and techniques for building distributed **network systems**, including examples in TCP/IP communications, ... (AN 130165), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Data Transmission **Systems** / General; **COMPUTERS** / Networking / Vendor Specific; **Computer networks**; Electronic data processing--Distributed processing

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

6. **Handbook of Green Information and Communication Systems**

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S.
Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green Information and Communications **Systems**. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green information and communication **systems** are covered from a network ... (AN 485200), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

7. **Wireless Technologies : Concepts, Methodologies, Tools and Applications**

By: Information Resources Management Association. Hershey, PA : IGI Global. 2012. eBook. (AN 396408), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless Communications; TECHNOLOGY & ENGINEERING / Radio; Wireless communication **systems**; Telecommunication

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

8. **Advances in Enterprise Information Technology Security**

By: Herrmann, Francine; Khadraoui, Djamel. Hershey [Pa.] : IGI Global. 2007. eBook. Description: "This book provides a broad working knowledge of all the major security issues affecting today's enterprise IT activities. Multiple techniques, strategies, and applications are thoroughly examined, presenting the tools to address opportunities in the field. It is an all-in-one reference for IT managers, network administrators, researchers, and students"--Provided by publisher. (AN 185367), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Security / General; **COMPUTERS** / Security / Networking; **COMPUTERS** / Security / Online Safety & Privacy; **Computer security**; Data protection; Business enterprises--**Computer networks**--Security measures; Information technology--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

9. **Complete Book of Remote Access : Connectivity and Security**

By: Kasacavage, Victor. Series: The Auerbach Best Practices Series. Boca Raton, Fla : Auerbach Publications. 2003. eBook. Description: As technology advances, the demand and necessity for seamless connectivity and stable access to servers and networks is increasing exponentially. Unfortunately the few books out there on remote access focus on Cisco certification preparation, one aspect of network connectivity or security. This text covers both--the enabling technology and how to make remote access secure. The definitive resource for network administrators and IT professionals implementing and maintaining remote access systems, The ... (AN 135484), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Networking / General; **COMPUTERS** / Security / General; **Computer networks**--Remote access; **Computer networks**--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

10. **Mobile and Wireless Communication Networks :**
IFIP TC6/WG6.8 Conference on Mobile and
Wireless Communication **Networks** (MWCN
2004), October 25-27, 2004, Paris, France

By: Belding-Royer, Elizabeth M.; Al Agha, Khaldoun; Pujolle, G.;
International Federation for Information Processing. Series: International
Federation for Information Processing, Vol. 162. New York : Springer, 2005.
eBook. (AN 133162), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications;
Wireless communication **systems**--Congresses; Mobile communication
systems--Congresses

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

11. **Absolute FreeBSD, 3rd Edition : The Complete
Guide to FreeBSD**

By: Michael W. Lucas, [N.p.] : No Starch Press, 2018. eBook. Description:
This updated edition of Michael W. Lucas's definitive volume on FreeBSD-
based **systems** adds coverage of modern disks, the ZFS filesystem IPv6,
redesigned jail and packaging **systems**, and virtualization, among dozens of
new features added in the last 10 years. FreeBSD is the muscle behind
companies like Netflix and EMC. Any place where someone does heavy
lifting on the Internet, you'll find FreeBSD. This newly revised edition of
Absolute FreeBSD brings FreeBSD's strengths to bear on your problems and
covers ... (AN 1627006), Database: eBook Index

Subjects: **COMPUTERS** / Operating **Systems** / UNIX; **COMPUTERS** /
System Administration / Linux & UNIX Administration

 [Full Text Finder](#) [USPTO Full Text Options](#)

12. **Rugged Embedded Systems : Computing in Harsh Environments**

By: Vega, Augusto; Bose, Pradip; Buyuktosunoglu, Alper. [Place of publication not identified] : Morgan Kaufmann, 2016. eBook. Description: **Rugged Embedded Systems: Computing in Harsh Environments** describes how to design reliable embedded **systems** for harsh environments, including architectural approaches, cross-stack hardware/software techniques, and emerging challenges and opportunities. A 'harsh environment' presents inherent characteristics, such as extreme temperature and radiation levels, very low power and energy budgets, strict fault tolerance and security constraints, etc. that challenge the **computer system** in its design and operation. ... (AN 1144177), Database: eBook Index

Subjects: **COMPUTERS** / Microprocessors; **COMPUTERS** / Intelligence (AI) & Semantics; **TECHNOLOGY & ENGINEERING** / Robotics; Fault-tolerant computing; **Computers--Reliability**



Full Text Finder

USPTO Full Text Options

13. Security issues in cloud environments: a survey.

By: Fernandes, Diogo; Soares, Lilliana; Gomes, João; Freire, Mário; Inácio, Pedro. *International Journal of Information Security*. Apr2014, Vol. 13 Issue 2, p113-170. 58p. Abstract: In the last few years, the appealing features of cloud computing have been fueling the integration of cloud environments in the industry, which has been consequently motivating the research on related technologies by both the industry and the academia. The possibility of paying-as-you-go mixed with an on-demand elastic operation is changing the enterprise computing model, shifting on-premises infrastructures to off-premises data centers, accessed over the Internet and managed by cloud hosting providers. Regardless of its advantages, the transition to this computing paradigm raises security concerns, which are the subject of several studies. Besides of the issues derived from Web technologies and the Internet, clouds introduce new issues that should be cleared out first in order to further allow the number of cloud deployments to increase. This paper surveys the works on cloud security issues, making a comprehensive review of the literature on the subject. It addresses several key topics, namely vulnerabilities, threats, and attacks, proposing a taxonomy for their classification. It also contains a thorough review of the main concepts concerning the security state of cloud environments and discusses several open research topics. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s10207-013-0208-7. (AN: 95064452), Database: Computer Source

Subjects: CLOUD computing security measures; **COMPUTER networks** in business enterprises; ELASTICITY (Economics); WEB services; CLOUD computing; MANAGEMENT

[PDF Full Text](#) (1.7MB) [USPTO Full Text Options](#)

14. Securing Cisco IP Telephony Networks

By: Akhil Behl. Series: Networking Technology: IP Communications. [N.p.] : Cisco Press. 2012. eBook. Description: The real-world guide to securing Cisco-based IP telephony applications, **devices**, and **networks** Cisco IP telephony leverages converged **networks** to dramatically reduce TCO and improve ROI. However, its critical importance to business communications and deep integration with enterprise IP **networks** make it susceptible to attacks that legacy telecom **systems** did not face. Now, there's a comprehensive guide to securing the IP telephony components that ride atop data **network** infrastructures--and thereby providing ... (AN 1597740). Database: eBook Index

Subjects: **COMPUTERS** / Networking / General



Full Text Finder

USPTO Full Text Options

15. Directory-enabled Networks

By: Gonçalves, Marcus. New York : McGraw-Hill Professional. 1999. eBook. (AN 12999). Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Information Technology; **COMPUTERS** / Computer Literacy; **COMPUTERS** / Computer Science; **COMPUTERS** / Data Processing; **COMPUTERS** / Machine Theory; **COMPUTERS** / Reference; **COMPUTERS** / Hardware / General; **Computer networks**

PDF Full Text

USPTO Full Text Options

Download

Table of Contents

Most Relevant Pages From This eBook

16. Using Microsoft Windows XP

By: Cowart, Robert; Knittel, Brian. Edition: Platinum ed. Indianapolis, Ind : Pearson Education, Inc. 2004. eBook. Description: Title from ebook title screen (viewed on Apr. 28, 2005). (AN 128872), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Apple (Mac OS & iOS); **COMPUTERS** / Operating **Systems** / Windows Desktop; **COMPUTERS** / Operating **Systems** / Windows Server; **COMPUTERS** / Operating **Systems** / DOS; **COMPUTERS** / **System** Administration / Windows Administration; Operating **systems** (**Computers**)

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

17. Principles of Computer System Design : An Introduction

By: Saltzer, J. H.; Kaashoek, Frans. Burlington, MA : Morgan Kaufmann. 2009. eBook. Description: Principles of Computer System Design is the first textbook to take a principles-based approach to the computer system design. It identifies, examines, and illustrates fundamental concepts in computer system design that are common across operating systems, networks, database systems, distributed systems, programming languages, software engineering, security, fault tolerance, and architecture. Through carefully analyzed case studies from each of these disciplines, it demonstrates how to apply these ... (AN 319653), Database: eBook Index

Subjects: **COMPUTERS** / Microprocessors; **Computer systems**; **System** design

 [Full Text Finder](#) [USPTO Full Text Options](#)

18. **Tech Terms : What Every Telecommunications
and Digital Media Professional Should Know**

By: Rutenbeck, Jeffrey B. Amsterdam : Routledge. 2006. eBook. Description: An avalanche of acronyms, terms-of-art, buzz words, and short-hand phraseology confronts today's busy communications professionals. Now in its 3rd edition, Tech Terms is an invaluable learning tool to help grasp key aspects of the television and video, PC hardware and software markets, multimedia authoring tools, and the exploding wireless Internet and mobile telecomputing worlds. With more than 1000 terms described in four sentences or less, Tech Terms is perfect the perfect desk reference. (AN 166759), Database: eBook Collection (EBSCOhost)

Subjects: LANGUAGE ARTS & DISCIPLINES / Communication Studies; Telecommunication--Dictionaries; Digital media--Dictionaries

[PDF Full Text](#) [EPUB Full Text](#) [USPTO Full Text Options](#)

[Download](#)

[Table of Contents](#)

[Most Relevant Pages From This eBook](#)

19. **Networking Explained**

By: Gallo, Michael A.; Hancock, Bill. Boston : Digital Press. 1999. eBook. Description: Networking Explained is aimed at computer professionals who have an interest in furthering their knowledge of the fundamental principles of networks and networking. It employs an easy to follow question and answer format. The questions are representative of those asked by people who are already in the computing field and are categorized hierarchically by subject so that busy readers who seek answers to specific questions in the heat of combat can find them easily. The answers are intended to give ... (AN 34052), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; Computer networks

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#)

[Most Relevant Pages From This eBook](#)

20. **Introduction to Multimedia Communications :
Applications, Middleware, Networking**

By: Rao, K. Ramamohan; Bojkovic, Z. S.; Milovanovic, Dragorad A.
Hoboken, N.J. : Wiley-Interscience. 2006. eBook. Description: A
comprehensive resource on multimedia communications. Covers recent
trends and standardization activities in multimedia communications, such as
layered structures, underlying theories and the current best design
techniques. Describes the convergence of various technologies including
communications, broadcasting, information technology, and home
electronics, and emerging new communication services and applications
resulting from the growth of the Internet and wireless technologies. Please go
to [www-ee.uta.edu/dip ...](http://www-ee.uta.edu/dip...) (AN 149077), Database: eBook Collection
(EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications;
Multimedia communications

PDF Full Text **USPTO Full Text Options** **Download**
Table of Contents Most Relevant Pages From This eBook

21. **Essential System Administration**

By: Frisch, AEleen. Series: A Nutshell Handbook. Edition: 2nd ed.
Sebastopol, CA : O'Reilly Media. 1995. eBook. (AN 24420), Database:
eBook Collection (EBSCOhost)

Subjects: COMPUTERS / System Administration / Linux & UNIX
Administration; Operating systems (Computers)

PDF Full Text **USPTO Full Text Options** **Download**
Table of Contents Most Relevant Pages From This eBook

22. Using NetWare 4.1

By: Lawrence, Bill. Edition: Special ed., 2nd ed. Indianapolis, Ind : Pearson Education, Inc. 1996. eBook. Description: Includes index. (AN 16010), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / General; Operating **systems (Computers)**

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

23. Trust in Cyberspace

By: Schneider, Fred B.; National Research Council (U.S.). Washington, D.C. : National Academies Press. 1999. eBook. (AN 854), Database: eBook Collection (EBSCOhost)

Subjects: **TECHNOLOGY & ENGINEERING** / Telecommunications; **BUSINESS & ECONOMICS** / Industries / Media & Communications; Internet--Security measures; Telecommunication policy--United States; **Computer networks**--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

24. Essential Windows NT System Administration

By: Frisch, Aeleen. Edition: 1st ed. Cambridge, Mass : O'Reilly Media. 1998. eBook. Description: This is a comprehensive guide to the management of Windows NT **systems**, covering issues such as security, performance tuning, fault tolerance, backups, printing, and networking. (AN 24652), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / **System** Administration / Windows Administration; Operating **systems (Computers)**

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

25. **Sams Teach Yourself UNIX System
Administration in 21 Days**

By: Ray, Joan; Ray, William. Indianapolis, Ind : Pearson Education, Inc.
1999. eBook. (AN 8199), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Apple (Mac OS & iOS);
COMPUTERS / Operating **Systems** / Windows Desktop; **COMPUTERS** /
Operating **Systems** / Windows Server; **COMPUTERS** / Operating **Systems** /
DOS; **COMPUTERS** / **System** Administration / Windows Administration;
Operating **systems**

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

26. **Special Edition Using Unix**

By: Kuo, Peter. Edition: Special ed., 3rd ed. Indianapolis, Ind : Pearson
Education, Inc. 1998. eBook. Description: Includes Index. (AN 16024),
Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Virtualization;
COMPUTERS / Utilities; **COMPUTERS** / **System** Administration / General;
Operating **systems** (**Computers**)

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

27. **Practical UNIX and Internet Security**

By: Garfinkel, Simson; Spafford, Gene. Series: **Computer Security**. Edition:
2nd ed., expanded & updated. Bonn : O'Reilly Media. 1996. eBook. (AN
24630), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Security / General; **COMPUTERS** / Operating
Systems / UNIX; Operating **systems** (**Computers**); **Computer** security;
Internet--Congresses

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

28. UNIX Unleashed

By: Burk, Robin. Edition: 3rd ed. Indianapolis, IN : Pearson Education, Inc. 1998. eBook. Description: Includes index. (AN 8211), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Virtualization;
COMPUTERS / Utilities; **COMPUTERS** / **System** Administration / General;
Operating **systems** (**Computers**)

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

29. Using Netware 5.0

By: Kuo, Peter; Pence, John; Specker, Sally. Edition: Special ed. Indianapolis, Ind : Pearson Education, Inc. 1998. eBook. (AN 16011), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Virtualization;
COMPUTERS / Utilities; **COMPUTERS** / **System** Administration / General;
Operating **systems** (**Computers**)

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

30. Using Linux

By: Tackett, Jack; Burnett, Steven Forrest. Edition: 4th ed., special ed. Indianapolis, Ind : Pearson Education, Inc. 1998. eBook. Description: Includes index. (AN 8177), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Operating **Systems** / Apple (Mac OS & iOS);
COMPUTERS / Operating **Systems** / Windows Desktop; **COMPUTERS** /
Operating **Systems** / Windows Server; **COMPUTERS** / Operating **Systems** /
DOS; **COMPUTERS** / **System** Administration / Windows Administration;
Operating **systems** (**Computers**)

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

[EBSCO Support Site](#) | [Privacy Policy](#) | [Terms of Use](#) | [Copyright](#) | [Contact Us](#)

powered by *EBSCOhost*

© 2019 EBSCO Industries, Inc. All rights reserved.



Internet isolation for avoiding internet security threats



Sign in

All

News

Images

Videos

More

Settings

Tools

About 7,660 results (0.38 seconds)

Internet isolation for avoiding internet security threats

www.google.com/patents/US20130318594



App. - Filed Jan 27, 2012 - Published Nov 28, 2013 - Robert B. Hoy - L-3 Communications Corporation

The virtual guest system is separated and completely isolated by an internal firewall from the host, and ... Internet isolation for avoiding internet security threats ...

Overview · Related · Discuss

Internet isolation for avoiding internet security threats

www.google.com/patents/WG2012103517A1?ci=en



App. - Filed Jan 27, 2012 - Published Aug 2, 2012 - Robert B. HOY - L-3 Communications Corporation

This virtual guest system is separated and completely isolated by an internal firewall ... Internet isolation for avoiding internet security threats ...

Overview · Related · Discuss

Internet isolation for avoiding internet security threats

www.google.com/patents/CA2825811A1?ci=en



App. - Filed Jan 27, 2012 - Published Aug 2, 2012 - Robert B. Hoy - L-3 Communications Corporation

A host computer supports a virtual guest system running thereon. The host system has a firewall that prevents it from communicating directly ...

Overview · Related · Discuss

System and method for access management and security protection for ...

www.google.com/patents/US20100251329



App. - Filed Mar 24, 2010 - Published Sep 30, 2010 - Coach Wei - Yottaa, Inc.

Access management is not only about preventing unwanted access, but also about access rules and policies. ... Some common Internet security issues include the following: ...

Corporation Internet isolation for avoiding internet security threats.

Overview · Related · Discuss

Methods for firewall protection of mass-storage devices

www.google.com/patents/US8806604



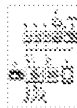
Grant - Filed Jun 28, 2007 - Issued Aug 12, 2014 - Ittai Golde - Sandisk II Ltd.

A method for protecting a host system from information security risks posed by a ... network architecture, and more specifically herein, the Internet protocol (IP).

Overview · Related · Discuss

System, method, and computer program product for managing a ...

www.google.com/patents/US20130246621



App. - Filed Jul 30, 2008 - Published Sep 19, 2013 - Efrain Ortiz, Jr. - Efrain Ortiz, Jr.

... are managed for security purposes, such as for preventing unwanted ... a wireless network, a wide area network (WAN) such as the Internet, ...

Overview · Related · Discuss

Network Protection from Cyber Attacks

www.google.com/patents/US20160134643



App. - Filed Jan 15, 2016 - Published May 12, 2016 - Paul Giura - At&T Intellectual Property I, L.P.

Advanced Persistent Threats (APTs) are one of the fastest growing information security threats that organizations face today. The goals of an APT are typically to ...

Overview · Related · Discuss

Web browser operating system

www.google.com/patents/US7836303

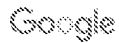


Grant - Filed Dec 9, 2005 - Issued Nov 16, 2010 - Henry M. Levy - University Of Washington

Despite many attempts to retrofit isolation and security, the browser's original roots ... that provides access to private resources and a restricted subset of the Internet, ... isolates the Web applications from each other, preventing resource sharing or ... browser architecture;

(1) its safety and effectiveness in containing threats, ...

Overview · Related · Discuss



Internet isolation for avoiding internet security threats

[Sign in](#)

Method and system for preventing and detecting security threats ... Internet-based retail interface provides a system by which the third-party application ...
[Overview](#) · [Related](#) · [Discuss](#)

Virus-resistant computer with data interface for filtering data

www.google.com/patents/US20070220187



App. - Filed Mar 20, 2006 - Published Sep 20, 2007 - Lawrence Kates - Lawrence Kates
This will help prevent unwanted file types and viruses from being transferred to or from the ... Corporation Internet isolation for avoiding internet security threats.
[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 [Next](#)

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)



1. INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

Patent Application: 15/910734. Filed: March 02, 2018. Published: July 5, 2018. , Database: USPTO Patent Applications

Abstract: A host computer supports a virtual guest system running thereon. The host system has a firewall that prevents it from communicating directly with the **Internet**, except with predetermined trusted sites. The virtual guest runs on a hypervisor, and the virtual guest comprises primarily a browser program that is allowed to contact the **Internet** freely via an **Internet** access connection that is completely separate from the host computer connection, such as a dedicated network termination point with its specific **Internet** IP address, or by tunneling through the host machine architecture to reach the **Internet** without exposing the host system. The virtual guest system is separated and completely isolated by an internal firewall from the host, and the guest cannot access any of the resources of the host computer, except that the guest can initiate cut, copy and paste operations that reach the host, and the guest can also request print of documents. The host can transfer files to and from a virtual data storage area accessible by the guest by manual operator action. No other transfer of data except these user initiated actions is permitted.

AN: edspap.20180191684

USPTO Full Text Options

2. **Internet isolation for avoiding internet security threats**

By: Hoy, Robert B.; Fenkner, Mark; Farren, Sean W. US Patent: 9,942,198.
Filed: January 27, 2012. Issued: April 10, 2018. , Database: USPTO Patent Grants

Abstract: A host computer supports a virtual guest system running thereon. The host system has a firewall that prevents it from communicating directly with the **Internet**, except with predetermined trusted sites. The virtual guest runs on a hypervisor, and the virtual guest comprises primarily a browser program that is allowed to contact the **Internet** freely via an **Internet** access connection that is completely separate from the host computer connection, such as a dedicated network termination point with its specific **Internet** IP address, or by tunneling through the host machine architecture to reach the **Internet** without exposing the host system. The virtual guest system is separated and completely isolated by an internal firewall from the host, and the guest cannot access any of the resources of the host computer, except that the guest can initiate cut, copy and paste operations that reach the host, and the guest can also request print of documents. The host can transfer files to and from a virtual data storage area accessible by the guest by manual operator action. No other transfer of data except these user initiated actions is permitted.

AN: edspgr.09942198

USPTO Full Text Options

3. INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

Patent Application: 13/981896. Filed: January 27, 2012. Published: November 28, 2013. , Database: USPTO Patent Applications

Abstract: A host computer supports a virtual guest system running thereon. The host system has a firewall that prevents it from communicating directly with the Internet, except with predetermined trusted sites. The virtual guest runs on a hypervisor, and the virtual guest comprises primarily a browser program that is allowed to contact the Internet freely via an Internet access connection that is completely separate from the host computer connection, such as a dedicated network termination point with its specific Internet IP address, or by tunneling through the host machine architecture to reach the Internet without exposing the host system. The virtual guest system is separated and completely isolated by an internal firewall from the host, and the guest cannot access any of the resources of the host computer, except that the guest can initiate cut, copy and paste operations that reach the host, and the guest can also request print of documents. The host can transfer files to and from a virtual data storage area accessible by the guest by manual operator action. No other transfer of data except these user initiated actions is permitted.

AN: edspap.20130318594

USPTO Full Text Options

4. Deriving Cyber Security Risks from Human and Organizational Factors - A Socio-technical Approach.

By: McEvoy, Thomas Richard; Kowalski, Stewart James. *Complex Systems Informatics & Modeling Quarterly*. Mar/Apr2019, Issue 18, p47-64. 18p.

Abstract: Cyber security risks are socio-technical in nature. They result not just from technical vulnerabilities but also, more fundamentally, from the degradation of working practices over time - which move an organization across the boundary of secure practice to a place where attacks will not only succeed, but also have a significantly greater impact on the organization. Yet current risk analysis and management methodologies are not designed to detect these kinds of systemic risks. We present an approach, devised in the field, to deriving these risks - using a qualitative research methodology, akin to grounded theory, but based on preset coding descriptors. This allows organizational and individual behavior identified during interviews, observations or document research to be thematically analyzed, collated and mapped to potential risks, linked to poor working practices. The resulting risk factors can be linked together forming "risk narratives", showing how the degradation of working practices in one part of the organization can contribute to undermining its ability to respond to cyber security threats in another part of the organization. [ABSTRACT FROM AUTHOR] DOI: 10.7250/csimq.2019-18.03. (AN: 136234486), Database: Engineering Source

Subjects: INTERNET security; ORGANIZATIONAL behavior; ICE shelves; QUALITATIVE research methodology; SYSTEMIC risk (Finance); RISK assessment; COMPUTER crime prevention

PDF Full Text (2.5MB) USPTO Full Text Options

5. **Security, privacy and trust in Internet of Things:
The road ahead**

By Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A.. In *Computer Networks*. 15 January 2015 76:146-164 Language: English. DOI: 10.1016/j.comnet.2014.11.008 Abstract: **Internet** of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains. In this scenario, the satisfaction of **security** and privacy requirements plays a fundamental role. Such requirements include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of **security** and privacy policies. Traditional **security** countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arises scalability issues; therefore a flexible infrastructure is needed able to deal with **security threats** in such a dynamic environment. In this survey we present the main research challenges and the existing solutions in the field of IoT **security**, identifying open issues, and suggesting some hints for future research. (AN: S1389128614003971), Database: ScienceDirect

Subjects: Internet of Things; **Security**; Privacy; Trust



Full Text Finder

USPTO Full Text Options

6. CLOUD COMPUTING: MAJOR CHALLENGES AND COUNTER ACTS.

By: Ashraf, Arjmand; Jawad, M. Abdul. *International Journal of Advanced Research in Computer Science*, Mar/Apr2018, Vol. 9 Issue 2, p618-625, 8p

Abstract: Although Cloud Computing has remarkably provided us easy accessible, manageable and maintainable resources at effective costs, but due to the fact that all or multiple users are allocated with the similar resources present **security threats** to the cloud subscribers. It is well known fact that in cloud paradigm, the data and applications are always under the control of third party, which give rise to serious concerns among the cloud subscribers. Cloud computing attracts the attention of research community due to its potential to provide tremendous benefits to the industry and cloud subscribers, but it lingers because of the **security**, privacy, and trust issues with Cloud subscribers. If Cloud Service Provider's (CSP's) are being able to provide efficient **security** tools, the utilization of services will rise exponentially and it will soon become globally accepted computing. This paper provides state of the art of major **security** challenges in the cloud paradigm and the countermeasures to counteract with the **security** breaches. [ABSTRACT FROM AUTHOR]; DOI: 10.26483/ijarcs.v9i2.5861; (AN 130548878), Database: Applied Science & Technology Source

Subjects: Cloud computing; **Internet** service providers; Client/server computing; Computer network architects; Data warehousing; Wired Telecommunications Carriers; All Other Telecommunications; Other telecommunications; Data Processing, Hosting, and Related Services

[PDF Full Text \(370KB\)](#) [USPTO Full Text Options](#)

7. A stealth monitoring mechanism for cyber-physical systems

By Graveto, Vitor; Rosa, Luís; Cruz, Tiago; Simões, Paulo. In *International Journal of Critical Infrastructure Protection*. March 2019 24:126-143
Language: English. DOI: 10.1016/j.ijcip.2018.10.006 Abstract: Supervisory Control and Data Acquisition (SCADA) systems, which are often used in several types of Essential Systems and Critical Infrastructures, depend on control devices such as Programmable Logic Controllers, Remote Terminal Units and Intelligent Electronic Devices. Such devices, which are deployed at the edge of the SCADA infrastructure, directly interface with the physical processes under control. They are often based on embedded systems with limited capabilities and exposed to significant security and safety-related risks, as demonstrated by past incidents such as Stuxnet. However, despite the recognized relevance of those edge devices, they usually lack monitoring mechanisms able to detect device anomalies and/or cyber-physical threats. In this paper we propose a novel approach for stealth monitoring of those control devices, for purposes of security and safety management. This approach builds on cost-effective probes, which we designate as Shadow Security Units (SSU), directly attached to the monitored control devices. This privileged positioning enables the direct and fine-grained observation of both physical inputs/outputs (i.e. the physical processes under control) and network communication flows – allowing the exploitation of various novel monitoring approaches able to address sophisticated security threats not noticeable otherwise. Moreover, the SSU approach is not limited to SCADA scenarios, being also applicable to similar domains such as the Internet of Things (IoT), Avionics and Self-Driving systems. (AN: S1874548218300672), Database: ScienceDirect

Subjects: Safety and security monitoring; SCADA; Anomaly detection; Industrial automation and control systems



Full Text Finder

USPTO Full Text Options

8. Analysis of physical and cyber **security**-related events in the chemical and process industry.

By: Moreno, Valeria Casson; Reniers, Genserik; Salzano, Ernesto; Cozzani, Valerio. *Process Safety & Environmental Protection: Transactions of the Institution of Chemical Engineers Part B*. May2018, Vol. 116 Issue Part B, p621-631. 11p. Abstract: **Security threats** are becoming an increasing concern for chemical sites and related infrastructures where relevant quantities of hazardous materials are processed, stored or transported. In the present study, **security** related events that affected chemical and process sites, and related infrastructures, were investigated. The aim of the study is to frame a clear picture of the **threats** affecting the chemical and process industry, and to issue lessons learnt from past events. A database of 300 **security**-related accidents was developed and populated, starting from European and American sources. **Threat** categories that caused such events were identified and analyzed. The attack modes were investigated. Important differences were found with respect to geographical areas and industrial sectors affected. The use of explosives (both military and improvised explosive devices) is by far the more frequent attack mode, although armed attacks and arson are also frequent events and may result in an in-depth penetration of the attackers. In recent years, cyber-attacks are also posing important **threats**. Lessons learnt call for the implementation of a specific **security** management system in the chemical and process industry, aiming at the physical and cyber protection of industrial sites. [ABSTRACT FROM AUTHOR] DOI: 10.1016/j.psep.2018.03.026. (AN: 130426201), Database: Environment Complete

Subjects: Industrial safety; Chemical industry; Risk assessment; Chemical (except agricultural) and allied product merchant wholesalers; Other Chemical and Allied Products Merchant Wholesalers; All Other Basic Organic Chemical Manufacturing; Cyclic Crude, Intermediate, and Gum and Wood Chemical Manufacturing; Wired Telecommunications Carriers; **Internet** Publishing and Broadcasting and Web Search Portals; Cyberterrorism; **Internet security**

PDF Full Text (6.7MB) USPTO Full Text Options

9. The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity.

By: Zhang-Kennedy, Leah; Chiasson, Sonia; Biddle, Robert. *International Journal of Human-Computer Interaction* , 2016, Vol. 32 Issue 3, p215-257, 43p, 1 Illustration, 2 Diagrams, 12 Charts, 2 Graphs Abstract: Although computer security technologies are the first line of defense to secure users, their success is dependent on individuals' behavior. It is therefore necessary to persuade users to practice good computer security. This interview analysis of users' conceptualization of security password guessing attacks, antivirus protection, and mobile online privacy shows that poor understanding of security threats influences users' motivation and ability to practice safe behaviors. An online interactive comic series called Secure Comics was designed and developed based on instructional design principles to address this problem. An eye-tracking experiment suggests that the graphical and interactive components of the comics direct users' attention and facilitate comprehension of the information. In the evaluations of Secure Comics, results from several user studies show that the comics improve understanding and motivate positive changes in security management behavior. The implication of the findings to better understand the role of instructional design and persuasion in education technology are discussed. [ABSTRACT FROM AUTHOR]; DOI: 10.1080/10447318.2016.1136177; (AN 113304630), Database: Applied Science & Technology Source

Subjects: Computer security; Instructional systems design; Passwords (Computers); Antivirus software; Internet security; Security management; Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Persuasive technology; Internet privacy

Show all 17 images



[HTML Full Text](#) [PDF Full Text](#) (10.3MB)

[USPTO Full Text Options](#)

10. Security challenges with network functions virtualization

By Daghmehchi Firoozjaei, Mahdi; Jeong, Jaehoon (Paul); Ko, Hoon; Kim, Hyoungshick. In *Future Generation Computer Systems*. February 2017 67:315-324 Language: English. DOI: 10.1016/j.future.2016.07.002 Abstract: The advent of network functions virtualization (NFV) has revolutionized numerous network-based applications due to its several benefits such as flexibility, manageability, scalability, and **security**. By the software-based virtualization of network functions on a single infrastructure, NFV provides users with a framework that dynamically provisions various network services in a flexible manner. However, NFV faces several **security** challenges (e.g., multi-tenancy and live migration) which make it vulnerable to some cybersecurity attacks (e.g., side-channel attacks and shared resource misuse attacks). In this paper, we provide an overview of NFV, discuss potentially serious **security threats** on NFV and introduce effective countermeasures to mitigate those **threats**. Finally, we suggest some practical solutions to provide a trustworthy platform for NFV. (AN: S0167739X16302321), Database: ScienceDirect

Subjects: Network functions virtualization; Network **security**; Virtualized network function; **Security threats**

[Full Text Finder](#)[USPTO Full Text Options](#)

11. Authoritarianism and the Internet

By: Druzin, Bryan; Gordon, Gregory S.. In: *Law & Social Inquiry*, Vol. 43, Issue 4 (Fall 2018), pp. 1427-1457 (AN: edshol.hein.journals.lsocig43.68), Database: HeinOnline

Subjects: Illinois; Psychology/Sociology

[Full Text Finder](#)[USPTO Full Text Options](#)

12. Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies.

By: SUNDARARAJAN, Aditya; KHAN, Tanwir; MOGHADASI, Amir; SARWAT, Arif I.. *Journal of Modern Power Systems & Clean Energy*, May2019, Vol. 7 Issue 3, p449-467, 19p. Publisher: Springer Nature.; Abstract Synchrophasor devices guarantee situation awareness for real-time monitoring and operational visibility of smart grid. With their widespread implementation, significant challenges have emerged, especially in communication, data quality and cybersecurity. The existing literature treats these challenges as separate problems, when in reality, they have a complex interplay. This paper conducts a comprehensive review of quality and cybersecurity challenges for synchrophasors, and identifies the interdependencies between them. It also summarizes different methods used to evaluate the dependency and surveys how quality checking methods can be used to detect potential cyberattacks. This paper serves as a starting point for researchers entering the fields of synchrophasor data analytics and security. [ABSTRACT FROM AUTHOR]; (AN 136274856), Database: Complementary Index

Subjects: Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Computer systems design and related services (except video game design and development); Other Computer Related Services; DATA quality; INTERNET security; SITUATIONAL awareness; DATA security; PHASOR measurement; CYBER intelligence (Computer security)



Full Text Finder

USPTO Full Text Options

13. Uncertain environment, dynamic innovation capabilities and innovation strategies: A case study on Qihoo 360

By Wang, Wenke; Cao, Qilin; Qin, Li; Zhang, Yan; Feng, Tianli; Feng, Linyun. In *Computers in Human Behavior*. January 2017 Language: English. DOI: 10.1016/j.chb.2018.06.029 Abstract: This Paper studied the mutual influence between uncertain environment, enterprise dynamic innovation capabilities and innovation strategies and established a theoretical framework based on uncertain environment, enterprise dynamic innovation capabilities and innovation strategies. This framework will be used to analyze the support of an enterprise's dynamic innovation capabilities for its innovation strategies behaviors under the transition period of uncertain environment. Based on the theoretical framework, an in-depth study was conducted on the case of Qihoo 360's micro-innovation based on "free and secure" products. According to analysis of specific Qihoo 360 "micro-innovation", we understood that dynamic innovation capabilities are the support maintaining an enterprise's competitiveness. Furthermore, it was found that Qihoo 360 became the leading figure in the **internet security** industry by providing an "iteration process" of all products on a "non-payment" and "security" basis. This Paper contributed to the further enrichment of the connotations of dynamic innovation capabilities and analysis of the mechanism of micro-innovation strategy, and the dynamic supporting mechanism of enterprise dynamic innovation capabilities on its micro-innovation strategy is studied under the background of uncertainty environment. It provides theoretical support and practical guidance for **Internet** enterprises to carry out innovation activities in an uncertain environment. (AN: S0747563218303066), Database: ScienceDirect

Subjects: Uncertain environment; Dynamic innovation capabilities; Innovation strategies; Micro-innovation; Qihoo 360



Full Text Finder

USPTO Full Text Options

14. Computer and Information **Security** Handbook

By: Vacca, John R. Series: The Morgan Kaufmann Series in Computer **Security**. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network **threats**. Also imparts the skills and knowledge needed to identify and counter some fundamental **security** risks and requirements, including **Internet security threats** and measures (audit trails IP sniffing/spoofing etc.) and how to implement **security** policies and procedures. In addition, this book covers **security** and network ... (AN 248986), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / **Security** / General; Computer networks--**Security** measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

15. 150 Things You Should Know about **Security**

In *150 Things You Should Know about Security* Edition: Second Edition. 2018 :1-218 Language: English. DOI: 10.1016/B978-0-12-809485-3.00001-6 Abstract: Crime Prevention Through Environmental Design (CPTED) concepts have been proven to enhance community activities while reducing crime problems and are fundamental to traditional law enforcement values, in terms of helping the community to function properly. The seven overlapping strategies of CPTED are discussed. The questions that are to be answered during a CPTED assessment are listed. The benefits of CPTED planning, in addition to dealing with the reduction of crime and fear problems, are listed. There needs to be the right mix of people and technology for the overall **security** plan to be effective. Therefore, the role of access control and video surveillance in preventing crime is discussed. The authors discuss extensively about soft targets and the role of target-hardening in reducing crime. A **security** checklist, including 35 **security** checkpoints, to assist in risk assessment is provided. The role of physical **security** in health care environment is described. Lighting is the single most cost-effective deterrent to crime. Hence, the types of lighting, their sources, and goals are reviewed. Special attention is paid to the subject of active shooter/active assailant and how one should respond when an active shooter is in the vicinity. The authors have also provided a classification of fires and the selection of extinguishers based on the type of fire. Fraudulent activity is an issue for individuals and all types of business operations from the small mom-and-pop store to the large Fortune 50 operation. The goal of those initiating and committing the fraudulent activity is to gain some type of monetary benefit. The goal of the targeted operation is to identify the **threat** and to educate their associates to identify and to eventually block the **threat**. Therefore the authors have discussed the top ten fraud-related issues present today. (AN: B9780128094853000016), Database: ScienceDirect

Subjects: 10,080 pixel; 3 D's; 360 degree peephole; A Plus Paper Shredding; Access controls; Access risks; Active assailant; Active **security**; Active shooter; Actively check professional references; Activity program; Activity program support; Activity support; ADA requirements; Additional hours; Additional work; Adopt-a-student programs; AED; Age or marital status; Alarms; Alerts; All lives matter; Annealed glass; Anticipation; Appraisal of a crime risk; Approaches; Approved by UL; ASIS; ASIS School Safety and **Security** Council; Asphyxiation; Assaults; ATM; Audit; Auditing; Auditors; Audits/assessment/future; Authority; Bad management skills; Badge control; Benefits; Burglars; Best practices; Biometrics; Biometrics and access control to specific areas; Blue light phone; Blueprints and designs; Body cameras; Bollards or barricades closing down streets and controlling access; Broken; Browser-based user interface. Both the K3 and K5 integrate

the 90 terabytes of data; Building designs; Bullet-resistant glass; Bulletproof glass; Bullycide; Bullying; Bumper stickers; Bumps; Burglar; Burglar resistant; Bus accidents; Calling 911; Capital letters; Carelessness; CEO; Certification; Changing attitudes; Changing of climate control; Charley bar; Check criminal and credit histories; Chemical storage; Clear border; Communication; Communications and video surveillance; Community; Community awareness; Conducting investigations; Confident; Conflict; Consider integrity surveys; Construction sites; Contracts; Copper drains; COPS; CORI check; Corporate executives; CPR; CPTED; CPTED design; CPTED for 2017 and beyond; CPTED landscape principles; CPTED principles; CPTED principles and concepts; CPTED principles and strategies; CPTED, the second generation; CPTED, the third generation; Credentials; Crime analysis; Crime displacement; Crime pattern analysis; Crime problems; Crime rate; Crime risk; Criminal and civil law; Criminal assets; Cross-examination; Crowding; Crying; C-TPAT; Customs Trade Partnership Against Terrorism; Cybercrime; Data breach; Data center; Data **security**; Dedicated **security** personnel; Defensible space; Defensible space principles and concepts; Delay time; Deletion; Deposition; Depression; Designing for **security**; Deter; Deterrents; Developing **security** points; Digital closed-circuit television; Digital recording; Disabilities; Disaster response; Displacement of crime; Documentation; Doors; Drunk driver; Duty; Dynamic alarm management; Dynamic risk; Emergency command center; Emergency evacuation planning; Emergency light; Emergency management; Emergency planning/procedures; Encryption; Entrance; Entrapment; Environment; Environmental clues; Environmental **security**; Equipment requirements; Ethnic background and race; Evacuation; Evidence preservation; Excessive postage (usually postage stamps); Exit doors; Exterior physical characteristics; Exterior windows; Extortion; Extremely hazardous; Fear of crime; Federal information center; Fee-based training services; Felony; FEMA; Fences; Financial printouts; Fire; Fire alarm system; Fire and safety regulations and codes; Fire detection and suppression equipment; Fire drills; Fire prevention; Fire prevention plan; Fire safety; Fire suppression; Firearms; First aid; First aid training; Flashing yellow signs/lights; Floor safe; Floors; Formulation of partnerships; Fraud; Gates; Geographical juxtaposition; Geographical juxtaposition (wider environment); Glare; Glass; Goals; Good **security**; Good visibility; Graffiti; Guard house; Guard shack; Guards; Guidelines; Hallcrest report; Hand geometry; Handouts; Hazardous material; Hazardous materials substances and wastes; HD; Health; HIPPA; Holiday season; Holistic; Hospital residential treatment; HVAC systems; Identify assets; Identity fraud and credit/debit card fraud; Identity theft; IESNA; IFPO; Image and/or maintenance; Image management; Informal organization; Informant; Infrastructure protection; Inge Sebyan Black; Ingestion; Inhalation; Injection; Inland regional center; Installation services; Insufficient information; Insurance coverage; Insurance forms and reports; Integrated **security** systems design; Intent; Interior; Interior/exterior layout; **Internet**-connected;

Intervention; Intrusion; Intrusion alarm system; Intrusion alarms and signage of alarms; Intrusion detection systems; Intuitive; Investigations; IP cameras; ISO; Key control; Lack of awareness; Laminated glass; Land use; Landscape **security** principles; Laptop computers; Larceny; Layout; Legal aspects; Legal authority; Letter bombs; Liability; Liaison; Life safety and fire prevention; Lighting; Lighting that meets standards and design by increased visibility; Lights; Lights burnt out; Limits; Local emergency management; Locks; Loss of self-esteem; Lower-case letters; Lows power; Magnetic stripe cards; Maintenance; Malicious destruction of property; Management systems requirements; Man-made disasters; Marketing and sales data; Mentally challenged; Mentoring programs; Merchandise; Mergers; Metal on roof tops; Methods of operation [typically called standard operating procedures (SOPs) and post orders]; Michael Fagel; Minimum standards; Misdemeanor; Missing or exploited children; Misspellings of common words; Monitoring equipment; Digital recording equipment; Multi-screen; Mutual aid association; Name-calling; Natural access; Natural access control; Natural barriers; Natural disasters; Natural surveillance; Neighborhood watch concepts and community involvement; Networks; NFPA; NFPA 101; NFPA ~~909~~; NFPA codes; NIMS; Non-random; Non-value-adding work; Numbering system; Numbers; OIP; Ongoing maintenance; On-site probation officers; Open hands; Openings; Order maintenance; Organization; Organizational resilience; OSHA standards; Overhead doors; Padlocks and door locks and peepholes; Pan and tilt; Pandemics; Panic and barrier alarms; Parking garages; Parking lots; Passive **security**; Passwords; People; Perimeter; Perimeter **security**; Perimeter walls; Personnel records and files; Physical deterrence; Physically challenged; Places of worship; Planners; Planning; Plastic glazing; Plexiglas; Police officer; Police powers; Policies; Policies and procedures; Poor/low morale; Portable alarms; Post orders; PowerPoints; Practice; Preparedness and continuity; Pre-recorded messages; President; Prevention; Prioritize; Probable cause; Procedures; Process error; Product failure; Product **security**; Production schedules; Professionalism; Proper protection to works on display; Proprietary information; Protection of depth; Protection of sensitive information; Protection officer; Protective clothing; Protective coverings; Protective lighting; PSIM stands for physical **security** information management; Purchases; Pure risk; Qualifications; Random; Rape; Reasonableness of the privacy expectation; Recognition; Recordkeeping; Reduce crime; Regulations; Relations with law enforcement; Religion; Remote starters; Reporting; Residential **security**; Risk; Risk assessment; Risk manager; Robbery; ROI; Roll-up window shutters; Roof access; Roofs; SSN; Sabotage; Safe; Safe areas; Safe schools; Safety; Safety glass; Safety issues; Sarbanes-Oxley; Saturday detention; School administrator/employer ratified; Schools; Secret information; **Securities** and Exchange Commission; **Security**; **Security** assessments; **Security** awareness; **Security** management; **Security** officer; **Security** officers checklist; **Security threats**; Server room; Setting specifications and getting

bids; Sexual harassment; Shutters; Signage; Sinkholes; Situational crime prevention; Situational crime prevention principles and concepts; Skilled; smart cards; Smash and grab attackers; Social media; Soft targets hardening 101; Soft targets versus hard targets; Software; Solutions; Space; Space design; Span of control; Spin the dial; Stan Carter; Standards; Standby; State department; Stop and think; Storms; Strategies; Strategy; Streetlight; Streetlighting; Stress; Stress on the job; Structural barriers; Student courts; Subcontractors; Suicide; Support; Survey; Suspicion of a crime; Symbols; Systems; Target hardening; Target hardening strategies; Target hardening versus soft targets; Taunting; Technology; Tempered glass; Territorial reinforcement; Terrorism; Terrorist attacks; Testifying; The concept; The environment; The initiation of an action; The Montreux Document; The operational **security** plan; Theft of supplies; There are seven overlapping strategies in CPTED; Thomas Norman; **Threats**; **Threats** of layoffs are all additional contributors to stress; Tires; Training; Transportation **security**; Trapped; Types of tasks/work; UL; UL codes; Undercover; Uniforms; Unsafe activities; Urban problems; US Department of Justice; Use of badges; Use of Force; Vacation; Value-adding work; Vendors; Verbal de-escalation; Victim sullen and isolated; Video; Video analytics; Video analytics and thermal cameras; Video surveillance; Violation of law; Visitors; Visual aids; Voice data; Wall safe; Walls; Waste; Weigand cards; Windows; Wired glass



Full Text Finder

USPTO Full Text Options

16. Risk and the Small-Scale Cyber **Security** Decision Making Dialogue--a UK Case Study.

By: Osborn, Emma; Simpson, Andrew. *Computer Journal*, Apr2018, Vol. 61 Issue 4, p472-495, 24p. Publisher: Oxford University Press / USA.; Abstract Despite a long-standing understanding that developments in personal and cloud computing practices would change the way we approach **security**, small-scale IT users (SSITUs) remain ill-served by existing cyber **security** practices. This paper discusses results from a survey that considered (in part) cyber **security** decisions made by SSITUs. We determine that SSITUs are focusing on easy-to-implement technical measures, leading to a disconnect between the **security** implemented and any risks identified; available resources, knowledge, prioritization of business processes, reduced system control and a lack of **threat** intelligence all combine to limit the ability to make cyber **security** decisions; and assessing risk in SSITUs will not lead to sufficient investment to mitigate risks for risk-holding stakeholders in the supply chain. We conclude that the constraints faced by SSITUs have far greater impact on the decisions they make than either our risk-holding, or **security**-providing, participants may have anticipated. Any limitations faced by SSITUs as they make their **security** decisions will have a significant impact on both the measures they are able to apply and the **security** of the supply chain as a whole. [ABSTRACT FROM AUTHOR]; (AN 128782999), Database: Complementary Index

Subjects: Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; Data Processing, Hosting, and Related Services; **INTERNET security**; **COMPUTER security**; INFORMATION technology; CYBERTERRORISM; CLOUD computing; DATA protection

Linked Full Text USPTO Full Text Options

17. Practical UNIX and Internet Security

By: Garfinkel, Simson; Spafford, Gene. Series: Computer Security. Edition: 2nd ed., expanded & updated. Bonn : O'Reilly Media, 1996. eBook. (AN 24630). Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / General; COMPUTERS / Operating Systems / UNIX; Operating systems (Computers); Computer security; Internet--Congresses

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

18. SEC Cybersecurity Guidelines: Insights Into the Utility of Risk Factor Disclosures for Investors.

By: Morse, Edward A.; Raval, Vasant; Wingender Jr., John R. *Business Lawyer*. 12/1/2017, Vol. 73 Issue 1, p1-34. 34p. 5 Charts. Abstract: In October 2011, the SEC issued new guidelines for disclosure of cybersecurity risks. Some firms responded to these guidelines by issuing new risk factor disclosures. This article examines the guidelines and cybersecurity disclosures in the context of existing laws governing securities regulation. It then examines empirical results from firm disclosures following the new guidelines. Evidence shows a relatively small proportion of firms chose to modify their risk factor disclosures, with most firms choosing not to disclose any specific cybersecurity risk. Moreover, disclosing firms generally experienced significant negative stock market price effects on account of making new disclosures. Rather than viewing disclosure as a positive signal of management attentiveness, investors apparently viewed it as a cautionary sign. [ABSTRACT FROM AUTHOR] (AN: 127499189), Database: Business Source Complete

Subjects: Investment risk; Disclosure of information; Investor confidence; Public companies; Good faith (Law); United States. Securities & Exchange Commission; Regulation, Licensing, and Inspection of Miscellaneous Commercial Sectors; Internet security laws; Securities -- United States

[HTML Full Text](#) [USPTO Full Text Options](#)

19. **A Server-Side JavaScript Security Architecture for Secure Integration of Third-Party Libraries.**

By: van Ginkel, Neline; De Groef, Willem; Piessens, Frank; Massacci, Fabio.
Security & Communication Networks, 5/2/2019, p1-21, 21p Abstract: The popularity of the JavaScript programming language for server-side programming has increased tremendously over the past decade. The Node.js framework is a popular JavaScript server-side framework with an efficient runtime for cloud-based event-driven architectures. One of its strengths is the presence of thousands of third-party libraries which allow developers to quickly build and deploy applications. These very libraries are a source of **security threats** as a vulnerability in one library can (and in some cases did) compromise an entire server. In order to support the secure integration of libraries, we developed NODESENTRY, the first **security** architecture for server-side JavaScript. Our policy enforcement infrastructure supports an easy deployment of web hardening techniques and access control policies on interactions between libraries and their environment, including any dependent library. We discuss the design and implementation of NODESENTRY and present its performance and **security** evaluation. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/9629034; (AN 136199504), Database: Applied Science & Technology Source

Subjects: JavaScript (Computer program language); Cloud computing; Computer network **security**; Client/server computing; Libraries and Archives; Commercial and Institutional Building Construction; Libraries; Data Processing, Hosting, and Related Services; Libraries

[HTML Full Text](#) [PDF Full Text \(4MB\)](#) [USPTO Full Text Options](#)

20. Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications.

By: Lim, Hazel Si Min; Taelhagh, Araz. *Energies* (19961073). May2018, Vol. 11 Issue 5, p1062. 1p. Abstract: Amidst rapid urban development, sustainable transportation solutions are required to meet the increasing demands for mobility whilst mitigating the potentially negative social, economic, and environmental impacts. This study analyses autonomous vehicles (AVs) as a potential transportation solution for smart and sustainable development. We identified privacy and cybersecurity risks of AVs as crucial to the development of smart and sustainable cities and examined the steps taken by governments around the world to address these risks. We highlight the literature that supports why AVs are essential for smart and sustainable development. We then identify the aspects of privacy and cybersecurity in AVs that are important for smart and sustainable development. Lastly, we review the efforts taken by federal governments in the US, the UK, China, Australia, Japan, Singapore, South Korea, Germany, France, and the EU, and by US state governments to address AV-related privacy and cybersecurity risks in-depth. Overall, the actions taken by governments to address privacy risks are mainly in the form of regulations or voluntary guidelines. To address cybersecurity risks, governments have mostly resorted to regulations that are not specific to AVs and are conducting research and fostering research collaborations with the private sector. [ABSTRACT FROM AUTHOR] DOI: 10.3390/en11051062. (AN: 132396988), Database: Energy & Power Source

Subjects: AUTONOMOUS vehicles; **INTERNET security**; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers

[HTML Full Text](#) [PDF Full Text](#) (605KB)

[USPTO Full Text Options](#)

21. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.

By: Gartzke, Erik; Lindsay, Jon R. *Security Studies*. Apr-Jun2015, Vol. 24 Issue 2, p316-348. 33p. Abstract: It is widely believed that cyberspace is offense dominant because of technical characteristics that undermine deterrence and defense. This argument mistakes the ease of deception on the Internet for a categorical ease of attack. As intelligence agencies have long known, deception is a double-edged sword. Covert attackers must exercise restraint against complex targets in order to avoid compromises resulting in mission failure or retaliation. More importantly, defenders can also employ deceptive concealment and ruses to confuse or ensnare aggressors. Indeed, deception can reinvigorate traditional strategies of deterrence and defense against cyber threats, as computer security practitioners have already discovered. The strategy of deception has other important implications: as deterrence became foundational in the nuclear era, deception should rise in prominence in a world that increasingly depends on technology to mediate interaction. [ABSTRACT FROM AUTHOR] DOI: 10.1080/09636412.2015.1038188. (AN: 103363905), Database: Academic Search Complete

Subjects: INTERNET security; CYBERTERRORISM; COUNTERTERRORISM; DECEPTION; DISINFORMATION; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers

[HTML Full Text](#) [PDF Full Text](#) (158KB)

[USPTO Full Text Options](#)

22. An event-based platform for collaborative **threats** detection and monitoring

By Lodi, Giorgia; Aniello, Leonardo; Di Luna, Giuseppe A.; Baldoni, Roberto. In *Information Systems*. January 2014 39:175-195 Language: English. DOI: 10.1016/j.is.2013.07.005 Abstract: Organizations must protect their information systems from a variety of **threats**. Usually they employ isolated defenses such as firewalls, intrusion detection and fraud monitoring systems, without cooperating with the external world. Organizations belonging to the same markets (e.g., financial organizations, telco providers) typically suffer from the same cyber crimes. Sharing and correlating information could help them in early detecting those crimes and mitigating the damages. The paper discusses the Semantic Room (SR) abstraction which enables the development of collaborative event-based platforms, on the top of **Internet**, where data from different information systems are shared, in a controlled manner, and correlated to detect and timely react to coordinated **Internet-based security threats** (e.g., port scans, botnets) and frauds. In order to show the flexibility of the abstraction, the paper proposes the design, implementation and validation of two SRs: an SR that detects inter-domain port scan attacks and an SR that enables an online fraud monitoring over the Italian territory. In both cases, the SRs use real data traces for demonstrating the effectiveness of the proposed approach. In the first SR, high detection accuracy and small detection delays are achieved whereas in the second, new fraud evidence and investigation instruments are provided to law enforcement agencies. (AN: S0306437913001014), Database: ScienceDirect

Subjects: Collaborative information systems; Information systems monitoring; Event processing; **Security threats**; Fraud monitoring



Full Text Finder

USPTO Full Text Options

23. Dual cooperative RFID-telecare medicine information system authentication protocol for healthcare environments.

By: Benssalah, Mustapha; Djeddou, Mustapha; Drouiche, Karim. *Security & Communication Networks*, Dec2016, Vol. 9 Issue 18, p4924-4948, 25p
Abstract: Radio Frequency IDentification (RFID) technology is used in a wide variety of applications, more recently as a leading identification technology in healthcare environments. In the most recent years, this technology has been adopted for telecare medicine information system (TMIS) for authentication, safety, security, data confidentiality, and patient's privacy protection over public networks. TMIS is the bridge between patients at home and doctors at healthcare organizations that permits to validate the correctness of exchanged information between different actors of the system. Recently, several RFID and smart cards authentication schemes have been presented and suggested for the TMIS in the literature. These schemes try to resolve the security and privacy problems over insecure healthcare network environments by exploiting different cryptographic primitive's solutions. In this paper, we first highlighted the vulnerabilities of the most recent proposed protocol for TMIS in the literature and proposed attacks based on the weaknesses related to the misuse of the timestamp technique, the calculation of the reader request and tag response messages using the one-way hash function, which are not attentively scrutinized. Second, we propose an efficient dual RFID-TMIS mobile authentication protocol with high efficiency and security for healthcare systems. Our proposal is an improvement and extension of the protocol of Li et al., where we propose to associate the RFID technology with TMIS in the same authentication system to take advantages of both these two promising technologies. The performance analysis shows that our improved protocol could solve security weaknesses of the studied protocol and provide mobility, efficiency and is well suited for TMIS adoption in remote areas and low population density. Copyright © 2016 John Wiley & Sons, Ltd. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.1665; (AN 122199477), Database: Applied Science & Technology Source

Subjects: Telemedicine; Computer access control; Radio frequency identification systems; Internet protocols; Internet security; Information storage & retrieval system security measures; Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Electronic components, navigational and communications equipment and supplies merchant wholesalers

PDF Full Text (764KB) USPTO Full Text Options

24. What good cyber resilience looks like.

By: Hult, Fredrik; Sivanesan, Giri. *Journal of Business Continuity & Emergency Planning*. Winter2013/2014, Vol. 7 Issue 2, p112-125. 14p.

Abstract: Over the past few years, a rapidly increasing number of sophisticated cyber attacks targeting high-profile organisations have been reported in the media. With the growing realisation of the severity and scale of the cyber threat, many security leaders are now questioning the effectiveness of just meeting compliance with information security standards and IT security control frameworks - can compliance provide organisations with the assurance that they are effectively managing the risk from cyber attacks? While an organisation may be able to take a tick-box approach to adopting foundational security practices, will this ensure a genuine commitment to defending the organisation? This paper looks to bring a perspective on cyber resilience in the context of a paradigm shift from regulatory information security compliance to adversarial cyber security to articulate the attributes of a cyber-resilient organisation. The aim is to give executives tools to determine whether their organisation is cyber resilient and to illustrate what good cyber resilience looks like today. [ABSTRACT FROM AUTHOR] (AN: 94779801), Database: Business Source Complete

Subjects: Computer network security; Cyberterrorism; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; Internet security; Counterterrorism; Information technology security measures; Cyber intelligence (Computer security)

PDF Full Text (10.2MB) USPTO Full Text Options

25. **Method and system for preventing and detecting security threats**

By: Irdeto B.V. US Patent: 10242,184. Filed: November 05, 2017. Issued: March 26, 2019. , Database: USPTO Patent Grants

Abstract: A system and method is provided for implementing platform **security** on a consumer electronic device having an open development platform. The device is of the type which includes an abstraction layer operable between device hardware and application software. A secured software agent is provided for embedding within the abstraction layer forming the operating system. The secured software agent is configured to limit access to the abstraction layer by either blocking loadable kernel modules from loading, blocking writing to the system call table or blocking requests to attach debug utilities to certified applications or kernel components.

AN: edspgr.10242184

USPTO Full Text Options

26. Security in cloud computing: Opportunities and challenges

By Ali, Mazhar; Khan, Samee U.; Vasilakos, Athanasios V.. In *Information Sciences*. 1 June 2015 305:357-383 Language: English. DOI: 10.1016/j.ins.2015.01.025 Abstract: The cloud computing exhibits, remarkable potential to provide cost effective, easy to manage, elastic, and powerful resources on the fly, over the Internet. The cloud computing, upsurges the capabilities of the hardware resources by optimal and shared utilization. The above mentioned features encourage the organizations and individual users to shift their applications and services to the cloud. Even the critical infrastructure, for example, power generation and distribution plants are being migrated to the cloud computing paradigm. However, the services provided by third-party cloud service providers entail additional **security threats**. The migration of user's assets (data, applications, etc.) outside the administrative control in a shared environment where numerous users are collocated escalates the **security** concerns. This survey details the **security** issues that arise due to the very nature of cloud computing. Moreover, the survey presents the recent solutions presented in the literature to counter the **security** issues. Furthermore, a brief view of **security** vulnerabilities in the mobile cloud computing are also highlighted. In the end, the discussion on the open issues and future research directions is also presented. (AN: S0020025515000638), Database: ScienceDirect

Subjects: Cloud computing; Multi-tenancy; **Security**; Virtualization; Web services



Full Text Finder

USPTO Full Text Options

27. Trust and Risk in Internet Commerce

By: Camp, L. Jean. Cambridge, Mass : The MIT Press, 2000. eBook.

Description: As Internet-based commerce becomes commonplace, it is important that we examine the systems used for these financial transactions. Underlying each system is a set of assumptions, particularly about trust and risk. To evaluate systems, and thus to determine one's own risks, requires an understanding of the dimensions of trust: security, privacy, and reliability. In this book Jean Camp focuses on two major yet frequently overlooked issues in the design of Internet commerce systems—trust and risk. Trust ... (AN 34347). Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Science; Electronic commerce--
Security measures; Internet--Security measures; Business enterprises--
Computer networks--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

28. Administrator and Fidelity Based Secure Routing (AFSR) Protocol in MANET.

By: Singh, Rohit; Saha, Himadri Nath; Bhattacharyya, Debika; Banerjee, Pranab Kumar. *Journal of Computing & Information Technology*, 2016, Vol. 24 Issue 1, p31-43, 13p Abstract: The proliferation of mobile computing and communication devices are driving a revolutionary change in our information society. Among all the applications and services run by mobile devices, network connections and corresponding data services are without doubt the most demanded services by mobile users. A MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires, which makes it ideal for the present scenario. But, due to lack of any centralized infrastructure and access to trusted authorities, the security in MANET poses a huge threat. The prominent routing protocols we know are generally designed for environments where the nodes within a network are non-malicious. Due to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb its development. We propose a protocol for MANETs named "Administrator and Fidelity Based Secure Routing Protocol" (AFSR), which ensures secure routing through the network: by electing an Administrator node on the basis of Willingness and Fidelity, after which a node only communicates to that secure Admin node. This selection of secured admin nodes results in mitigation of various threats. We have evaluated our proposed protocol by simulating and comparing in GloMoSim. [ABSTRACT FROM AUTHOR]; DOI: 10.20532/cit.2016.1002634; (AN 114682357), Database: Applied Science & Technology Source

Subjects: Network routing protocols; Ad hoc computer networks; Mobile computing; Mobile communication systems; Internet; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; Wireless Telecommunications Carriers (except Satellite); Information society

PDF Full Text (2.2MB) USPTO Full Text Options

29. A SURVEY ON DELAY AND NEIGHBOR NODE MONITORING BASED WORMHOLE ATTACK PREVENTION AND DETECTION.

By: Bagade, Sudhir T.; Raisinghani, Vijay T.. *ICTACT Journal on Communication Technology*, Dec2016, Vol. 7 Issue 4, p1417-1426, 10p
Abstract: In Mobile Ad-hoc Networks (MANET), network layer attacks, for example wormhole attacks, disrupt the network routing operations and can be used for data theft. Wormhole attacks are of two types: hidden and exposed wormhole. There are various mechanisms in literature which are used to prevent and detect wormhole attacks. In this paper, we survey wormhole prevention and detection techniques and present our critical observations for each. These techniques are based on cryptographic mechanisms, monitoring of packet transmission delay and control packet forwarding behavior of neighbor nodes. We compare the techniques using the following criteria- extra resources needed applicability to different network topologies and routing protocols, prevention/detection capability, etc. We conclude the paper with potential research directions. [ABSTRACT FROM AUTHOR]; DOI: 10.21917/ijcl.2016.0209; (AN 120697897), Database: Applied Science & Technology Source

Subjects: Cyberterrorism; Counterterrorism; Data security; Internet security; Routing (Computer network management); Cryptography; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; Other Computer Related Services; Computer systems design and related services (except video game design and development)

PDF Full Text (257KB) USPTO Full Text Options

30. **Security and privacy issues for the network of the future.**

By: Marias, Giannis F.; Barros, João; Fiedler, Markus; Fischer, Andreas; Hauff, Harald; Herkenhoener, Ralph; Grillo, Antonio; Lentini, Alessandro; Lima, Luisa; Lorentzen, Charlott; Mazurczyk, Wojciech; Meer, Hermann; Oliveira, Paulo F.; Polyzos, George C.; Pujol, Enric; Szczypiorski, Krzysztof; Vilela, João P.; Vinhoza, Tiago T. V.. *Security & Communication Networks*, Sep2012, Vol. 5 Issue 9, p987-1005, 18p Abstract: ABSTRACT The vision towards the Network of the Future cannot be separated from the fact that today's networks, and networking services are subject to sophisticated and very effective attacks. When these attacks first appeared, spoofing and distributed denial-of-service attacks were treated as apocalypse for networking. Now, they are considered moderate damage, whereas more sophisticated and inconspicuous attacks, such as botnets activities, might have greater and far reaching impact. As the Internet is expanding to mobile phones and 'smart dust' and as its social coverage is liberalized towards the realization of ubiquitous computing (with communication), the concerns on security and privacy have become deeper and the problems more challenging than ever. Re-designing the Internet as the Network of the Future is self-motivating for researchers, and security and privacy cannot be provided again as separate, external, add-on, solutions. In this paper, we discuss the security and privacy challenges of the Network of the Future and try to delimit the solutions space on the basis of emerging techniques. We also review methods that help the quantification of security and privacy in an effort to provide a more systematic and quantitative treatment of the area in the future. Copyright © 2011 John Wiley & Sons, Ltd. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.384; (AN 79293922), Database: Applied Science & Technology Source

Subjects: Computer network security; Computer privacy; Ubiquitous computing; Internet security; Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Apocalypse; Quantitative research

[PDF Full Text \(312KB\)](#) [USPTO Full Text Options](#)

[EBSCO Support Site](#) | [Privacy Policy](#) | [Terms of Use](#) | [Copyright](#) | [Contact Us](#)

powered by EBSCOhost

© 2019 EBSCO Industries, Inc. All rights reserved.

Method and apparatus for **implementing** security policies in a **network**

V Giles, B Jemes - US Patent App. 10/896,676, 2006 - Google Patents

... 1) connected to another interface 210 of **network** control point **device** 200 b and corresponding to ... A **single** instance of this bubble type might contain the authoritative DNS servers for a ... **One** advantage of the above-described architecture is that the infrastructure may comprise a ...

☆ 99 Cited by 99 Related articles All 2 versions

System and method for **implementing network** security policies on a common **network** infrastructure

B Jemes, JM Brawn, J Garcia, M Milligan ... - US Patent ..., 2007 - Google Patents

... **network** control point interconnects bubble partitions, **network** control point **devices** within the **same network** control point ... 1 and 2 . Campus 1, 2, and 3 can be organized as four separate real ... enterprise will have **one** virtual backbone, and service providers may have **one** or more ...

☆ 99 Cited by 44 Related articles All 4 versions

Network session wall passively listening to communication session, with **use** of access rules, stops further communication between **network devices** by emulating ...

Z Dascalu - US Patent 5,958,015, 1999 - Google Patents

... **device** stops performing the other **devices** will automatically replace it, assuming that they have access to the **same network** segment ... of session wall **devices** located on a common **network** segment, further comprising the step of, when **one** of said ... WO (1), WO1998019250A1 (en ...

☆ 99 Cited by 153 Related articles All 2 versions

External access to protected **device** on private **network**

G Tredoux, X Xu, B Lyon, R Cain - US Patent App. 09/845,104, 2002 - Google Patents

... This can **create** two problems: [0039]. 1. Race conditions ... A server that associates cookie data with a URL is thus not guaranteed that it will receive the **same** data back ... **One** way of doing this is to prepend the unique identity of the private **network** to each cookie name (that is, place ...

☆ 99 Cited by 58 Related articles All 2 versions

System and method for increasing host visibility in **network** address translation environments

RG Culbilli, JM Earls - US Patent 7,684,394, 2010 - Google Patents

... at **least one** internal host located inside a **firewall** for the **network**; a dynamic Domain Name Service (DNS) server for creating a ... US (1). US7684394B1 (en ... Corporation, **Internet** server system, method of creating virtual machine of the **internet** server and method of starting the **same** ...

☆ 99 Cited by 116 Related articles All 2 versions

Method and apparatus for supporting communications between a computing **device** within a **network** and an external computing **device**

CP Dingman, P Mahadevan, JJ Ordille - US Patent 9,497,168, 2016 - Google Patents

... In a NAT, in addition to translating addresses, port numbers are also translated, thereby enabling the conservation of IP addresses (in the sense that more than **one** internal IP address could be translated to the **same** external IP ... FIG. 1 illustrates a symmetric NAT/**firewall** 100 ...

☆ 99 Cited by 358 Related articles All 4 versions

System and method for **implementing** a virtual backbone on a common **network** infrastructure

B Jemes, J Pape, J Garcia, M Milligan - US Patent App. 09/795,778, 2001 - Google Patents

... first and second known networks have unrestricted **network** connectivity to all other **network devices** within the **same** known **network** ... system as defined in claim 25. , wherein the first and second virtual backbones are **implemented** using **one** or more ... WO (1), WO2002069597A2 (en ...

☆ 99 Cited by 11 Related articles All 2 versions

System and method for **implementing** a bubble policy to achieve host and **network** security

B Jemes, JM Brawn, L Buch-Pedersen - US Patent 7,376,965, 2008 - Google Patents

... inter-bubble **device** and the **network** control point **device** **implement** the **same network** security policy ... Alternatively, each bubble might have **one** structured access list template divided into four rule ... 1. action=permit protocol=ip; source=10.1.0.0 source_mask=255.255.0.0; 2. action ...

☆ 99 Cited by 52 Related articles All 4 versions

Method, apparatus and system for virtualized peer-to-peer **proxy** services

S Grobman, CC Jones - US Patent 7,788,713, 2010 - Google Patents

... 1 illustrates **an** example of a typical virtual machine host **device** ("Host 100 ... Thus, for example, in **one** embodiment, if Host 420 desires to download the **same** OS patch previously ... **One** or more of these elements may be integrated together with the processor on a **single** package ...

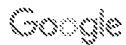
☆ ⓘ Cited by 103 Related articles All 4 versions ⓘ

Experiences from **an** IPv6-Only Network

J Arkkio, A Keranen - 2012 - tools.ietf.org

... NOT OK Skype NOT OK MSN NOT OK Webex NOT OK Sametime OK (NOW) Table 1. Instant Messaging ... and the increased failure rate matches that of IPv4 literal occurrence in the **same set** of top ... April 2012 DNS Discovery The state of DNS discovery continues to be **one** of the ...

☆ ⓘ Cited by 48 Related articles All 5 versions ⓘ





[All](#) [Videos](#) [News](#) [Images](#) [More](#)
[Settings](#) [Tools](#)

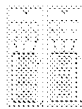
About 55,900 results (0.45 seconds)

Configuring interactions with a firewall service virtual machine

www.google.com/patents/US20150281178

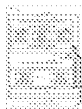

App. - Filed Mar 31, 2014 - Published Oct 1, 2015 - Chids Raman - Nicira, Inc.
 For a host that executes one or more guest virtual machines (GVIMs), some embodiments ...
 conceptually illustrates an electronic system ...
[Overview](#) · [Related](#) · [Discuss](#)

Combined firewalls

www.google.com/patents/US20090249470


App. - Filed Jan 5, 2009 - Published Oct 1, 2009 - Moshe Litvin - Moshe Litvin
 A method of providing a firewall to protect a set of virtual machines on a host node that is ...
 ... in particular firewalls for hosting systems with virtual machines, ... computers ...
 However, some embodiments may separately employ various elements ... same host ...
 node, each virtual machine has its own internal firewall 2310 and ...
[Overview](#) · [Related](#) · [Discuss](#)

Network isolation and identity management of cloned virtual machines

www.google.com/patents/US20100174811


App. - Filed Jan 5, 2009 - Published Jul 8, 2010 - Srikanth Srivathsan Musiri - Microsoft Corporation
 Accordingly, a technique for preserving network configuration data without creating ... The ...
 virtual computing systems are connected to the internal virtual ... A fence is created upon a ...
 physical host to isolate a virtual computing environment from ... network, or through an ...
 intermediary device, such as a firewall.
[Overview](#) · [Related](#) · [Discuss](#)

Virtual device context (VDC) integration for network services

www.google.com/patents/US9178912


Grant - Filed Nov 15, 2012 - Issued Nov 3, 2015 - Samar Sharma - Cisco Technology, Inc.
 Methods and apparatus are provided for virtual device context (VDC) ... switch and ...
 associated service nodes configured through a single processing system on ...
[Overview](#) · [Related](#) · [Discuss](#)

Distributed firewall security system for cloud computing environments

www.google.com/patents/US20150341318


App. - Filed Aug 4, 2015 - Published Nov 26, 2015 - Jaushin Lee - Zentara Systems, Inc.
 A traditional firewall system in enterprise network environments typically utilizes ...
 machines, a set of firewall rules are generated for each virtual machine in the ...
[Overview](#) · [Related](#) · [Discuss](#)

Replicating firewall policy across multiple data centers

www.google.com/patents/US20170004192


App. - Filed Jul 28, 2015 - Published Jan 5, 2017 - Uday MASUREKAR - Nicira, Inc.
 Each host is configured to host a set of data compute nodes (DCNs). ... virtual machine ...
 (VM) from a source host in a data center to a destination host in a different ...
[Overview](#) · [Related](#) · [Discuss](#)

Authenticated firewall tunneling framework

www.google.com/patents/US20020169980


App. - Filed Dec 1, 1998 - Published Nov 14, 2002 - David Brownell - David Brownell
 A user on an external host logs in into a firewall. ... Various tunnel classes are provided to ...
 configure tunnels in a variety of manners. ... Virtual ... Firewalls are used to screen traffic ...
 between "internal" networks and "external" networks (e.g. networks linked ... 2 is a block ...
 diagram that illustrates a computer system ... separate ...
[Overview](#) · [Related](#) · [Discuss](#)

System and method for managing resources in a virtual machine ...

www.google.com/patents/US20130283263


App. - Filed Apr 19, 2012 - Published Oct 24, 2013 - Walid H. Elernary - Incloud, Inc.
 A system and method for assigning attributes, such as directory or firewall attributes for ...
 virtual machines by a user over a ... the interface configured to receive inputs from the user ...
[Overview](#) · [Related](#) · [Discuss](#)

comprising ... Applications running within the VM will act just as they would if run on a "real" computer. ... separate ... internal ...
Overview · Related · Discuss

Virtual machine migration within a hybrid cloud system

www.google.com/patents/WO2017040326A1?cl=en

App. · Filed Aug 26, 2016 · Published Mar 9, 2017 · Gabriel Tarasuk-Levin · Vmware, Inc.
Hybrid cloud computing system 100 is configured to provide a common platform ... by an organization that is separate from a tenant that accesses the external cloud ... such as firewalls, network address translation (NAT), dynamic host configuration ... IP addresses for virtual data center 100 and one or more private internal ...
Overview · Related · Discuss

Methods and systems for orchestrating physical and virtual switches ...

www.google.com/patents/US20160294774

App. · Filed Apr 2, 2015 · Published Oct 6, 2016 · Marc Woolward · Varmour Networks, Inc.
4 illustrates an example computer system in accordance with various ... may be: a node, a communication node, a virtual machine, a container, and a host).
Overview · Related · Discuss

1 2 3 4 5 6 7 8 9 10 Next

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)



1. Destination Maternity Reports Third Quarter and First Nine Months Fiscal 2018 Results

Business Wire (English) , 12/11/2018 (AN 6CU92001071420181211005272),
Database: Newswires
[HTML Full Text](#)

2. Patent Application Titled 'Specially Programmed Computing Systems With Associated Devices Configured To Implement Centralized Services Ecu Based On Services Oriented Architecture And Methods Of Use Thereof' Published Online (USPTO 20190155650)

In: Computer Weekly News. June 12, 2019, 4072; NewsRX LLC Language: English. Abstract: 2019 JUN 12 (VerticalNews) -- By a News Reporter-Staff News Editor at Computer Weekly News -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (AN: edsgcl.588203953), Database: General OneFile

Subjects: Application programming interface; Application Programming Interface -- Methods

 [Full Text Finder](#) [USPTO Full Text Options](#)

3. BayCom Corp and Uniti Financial Corporation Announce Definitive Merger Agreement

Business Wire (English) , 12/10/2018 (AN 6CU92001071420181210005134),
Database: Newswires
[HTML Full Text](#)

4. Patent Application Titled 'Specially Programmed Computing Systems With Associated **Devices Configured To Implement** Centralized Services Ecu Based On Services Oriented Architecture And Methods Of Use Thereof Published Online (USPTO 20180349192)

In: Information Technology Newsweekly. Dec 25, 2018, 3783; NewsRX LLC
Language: English. Abstract: 2018 DEC 25 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly --
According to news reporting originating from Washington, D.C., by
VerticalNews journalists, a patent application [...] (AN: edsgcl.566846508),
Database: General OneFile



Full Text Finder

USPTO Full Text Options

5. Patent Issued for Specially Programmed Computing Systems With Associated **Devices Configured To Implement** Centralized Services ECU Based On Services Oriented Architecture And Methods Of Use (USPTO 10,191,777)

In: Journal of Engineering. Feb 11, 2019, 12982; NewsRX LLC Language:
English. Abstract: 2019 FEB 11 (VerticalNews) -- By a News Reporter-Staff
News Editor at Journal of Engineering -- From Alexandria, Virginia,
VerticalNews journalists report that a patent by the inventors Teshler, Dionis
[...] (AN: edsgcl.575697631), Database: Academic OneFile

Subjects: Application programming interface; Application Programming
Interface -- Methods; Application Programming Interface -- Reports;
Periodical publishing -- Intellectual property; Periodical publishing -- Methods;
Periodical publishing -- Reports



Full Text Finder

USPTO Full Text Options

6. SQN Sends Letter to Yelp Board of Directors

Business Wire (English) , 12/10/2018 (AN 6CU92001071420181210005360),

Database: Newswires

[HTML Full Text](#)

7. Patent Application Titled 'Specially Programmed Computing Systems with Associated **Devices Configured to Implement** Centralized Services Ecu Based on Services Oriented Architecture and Methods of Use Thereof Published Online (USPTO 20180189103)

In: Computer Weekly News. August 1, 2018, 2727; NewsRX LLC Language: English. Abstract: 2018 AUG 1 (VerticalNews) -- By a News Reporter-Staff News Editor at Computer Weekly News -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (AN: edsgcl.548089192), Database: General OneFile

Subjects: Application programming interface; Patent/copyright issue; Application Programming Interface -- Methods; Patents -- Methods



[Full Text Finder](#)

[USPTO Full Text Options](#)

8. Patent Application Titled 'Specially Programmed Computing Systems with Associated **Devices Configured to Implement** Centralized Services Ecu Based on Services Oriented Architecture and Methods of Use Thereof Published Online (USPTO 20180189103)

In: Computer Weekly News. July 25, 2018, 2530; NewsRX LLC Language: English. Abstract: 2018 JUL 25 (VerticalNews) -- By a News Reporter-Staff News Editor at Computer Weekly News -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (AN: edsgcl.547286536), Database: General OneFile

Subjects: Application programming interface; Patent/copyright issue; Application Programming Interface -- Methods; Patents -- Methods

 [Full Text Finder](#) [USPTO Full Text Options](#)

9. McLaren-Honda integrará la tecnología SDx de NTT Communications para el Gran Premio de Japón de Fórmula 1 de 2017

Business Wire (English) , 10/06/2017 (AN 6CU92001071420171006005264), Database: Newswires
[HTML Full Text](#)

10. Researchers Submit Patent Application, 'Method For Transmitting At Least One Ip Data Packet, Related System And Computer Program Product', for Approval (USPTO 20190052599)

In: Information Technology Newsweekly. March 5, 2019, 2608; NewsRX LLC
Language: English. Abstract: 2019 MAR 5 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly -- From
Washington, D.C., VerticalNews journalists report that a patent application by
the inventor Caserta, [...] (AN: edsgcl576714280), Database: General
OneFile

Subjects: Bridge/router; Internetworking **device**; ISDN router; Bridge/routers
-- Intellectual property; Bridge/routers -- Methods



Full Text Finder

USPTO Full Text Options

11. La scuderia McLaren-Honda si affida alle tecnologie SDx di NTT Communications per il Gran Premio del Giappone 2017 di Formula 1

Business Wire (English), 10/05/2017 (AN 6CU92001071420171005006109),
Database: Newswires
HTML Full Text

12. The Separation of Platforms and Commerce

By: Khan, Lina M.. In: Columbia Law Review, Vol. 119, Issue 4 (May 2019),
pp. 973-1098 (AN: edshol.hein.journals.clr119.26), Database: HeinOnline

Subjects: New York; General



Full Text Finder

USPTO Full Text Options

13. Bank-Customer Relationship and Provision of Quality Electronic Banking Services in Nigeria

By: Olowokere, Emmanuel Nimbe; Olufunmilayo, Adedeji, Abosede. In: Journal of Law, Policy and Globalization, Vol. 80, Issue 1 (2018), pp. 133-145 (AN: edshol.hein.journals.jawpglob80.18), Database: HeinOnline



Full Text Finder

USPTO Full Text Options

14. NTT Communications' SDx Technologies to be Adopted by McLaren-Honda for 2017 Formula 1 Japanese Grand Prix

Business Wire (English) , 10/05/2017 (AN 6CU92001071420171004006506), Database: News wires

HTML Full Text

15. Chapter 13 - Data Center Networks

In *Cloud Data Centers and Cost Modeling*, 2015 :497-576 Language: English. DOI: 10.1016/B978-0-12-801413-4.00013-1 Abstract: The content of this chapter is mainly divided into five topics: data center network (DCN) hardware, DCN terms, DCN metrics, DCN topologies, and characteristics of a cloud DCN. In terms of DCN topology, it starts with basic tree topology, which is highly recommended by one of the network equipment vendors, Cisco, and then the chapter discusses the fat tree, DCell, BCube, VL2, butterfly, and dragonfly topologies. Again, the main aim of these discussions is to highlight characteristics of each topology and associated costs for business needs. The section on cloud DCNs in this chapter covers four types of network: management, kernel, virtual machine, and virtualized storage. (AN: B9780128014134000131), Database: ScienceDirect

Subjects: Data center network topology; top of rack (ToR); aggregation; core router; high density switch; hub; bridge; routing protocol; gateway; node; diameter; dimension; radix; basic tree; fat tree; commodity switch fabric; end of row (EoR); recursive DCN topology; BCube; dragonfly



Full Text Finder

USPTO Full Text Options

16. Head in the Clouds, Head in the Sand: Federal Failure to Update Guidance on Computer Transactions in an International Context

By: Weaver, Logan S.. In: Washington Law Review, Vol. 93, Issue 4 (December 2018), pp. 2213-2246 (AN: edshol.hein.journals.washlr93.5f), Database: HeinOnline

Subjects: Washington; General



Full Text Finder

USPTO Full Text Options

17. Complete Book of Remote Access : Connectivity and Security

By: Kasacavage, Victor. Series: The Auerbach Best Practices Series. Boca Raton, Fla : Auerbach Publications. 2003. eBook. Description: As technology advances, the demand and necessity for seamless connectivity and stable access to servers and **networks** is increasing exponentially. Unfortunately the few books out there on remote access focus on Cisco certification preparation, **one** aspect of **network** connectivity or security. This text covers both-the enabling technology and how to make remote access secure. The definitive resource for **network** administrators and IT professionals implementing and maintaining remote access systems, The ... (AN 135484), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / Security / General; Computer **networks**--Remote access; Computer **networks**--Security measures

PDF Full Text

USPTO Full Text Options

Download

Table of Contents

Most Relevant Pages From This eBook

18. Cloud and Cluster Computing

By: Berman, Nan; Rivero, Georgetta. Delhi : Academic Studio. 2012. eBook.
Description: Chapter 1 - Enzyme Assay Chapter 2 - Alkaline Phosphatase
and Alanine Transaminase Chapter 3 - Amylase and Ceruloplasmin Chapter
4 - Glucose Chapter 5 - Bilirubin Chapter 6 - Human Chorionic Gonadotropin
Chapter 7 - Biomarker Chapter 8 - Mass Spectrometry Chapter 9 - C
--reactive Protein Chapter 10 - Ferritin Chapter 11 - DNA Assay Chapter 12 -
Protein Assay Chapter 13 - Drug Test Chapter 14 - Clonogenic Assay and
Bacteriological Water Analysis Chapter 15 - Immunostaining Chapter 16 -
MTT Assay, Nuclear ... (AN 446437), Database: eBook Collection
(EBSCOhost)

Subjects: COMPUTERS / Web / General; COMPUTERS / Networking /
Intranets & Extranets; Cloud computing

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

19. Innovations, Standards, and Practices of Web Services : Emerging Research Topics

By: Zhang, Liang-Jie. Hershey, PA : IGI Global. 2012. eBook. Description:
'This book provides a vital new compendium of the latest research topics in
the field of Web services, detailing the functions of service composition, and
the most relevant models that modify its construction'-- (AN 396409),
Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computerized Home & Entertainment; Web
services

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

20. **Materials and the Environment : Eco-informed
Material Choice**

By: Ashby, M. F. Edition: 2nd ed. Burlington : Butterworth-Heinemann. 2012. eBook. Description: Materials and the Environment: Eco-Informed Material Choice, Second Edition, is the first book devoted solely to the environmental aspects of materials and their selection, production, use and disposal, by **one** of the world's foremost materials authorities. It explores human dependence on materials and its environmental consequences and provides perspective, background, methods, and data for thinking about and designing with materials to minimize their environmental impact. Organized into 15 chapters, ... (AN 453829), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Materials Science / General; NATURE / Environmental Conservation & Protection; Materials--Environmental aspects

PDF Full Text	USPTO Full Text Options	Download
Table of Contents	Most Relevant Pages From This eBook	

21. **Computer and Information Security Handbook**

By: Vacca, John R. Series: The Morgan Kaufmann Series in Computer Security. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents information on how to analyze risks to your **networks** and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and **network** threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to **implement** security policies and procedures. In addition, this book covers security and **network** ... (AN 248988), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / Security / General; Computer **networks**--Security measures

PDF Full Text	USPTO Full Text Options	Download
Table of Contents	Most Relevant Pages From This eBook	

22. Renewable and Sustainable Energy II

By: Ren, Nanqi. Series: Advanced Materials Research, v. 512-515. Dürnten-Zürich, Switzerland : Trans Tech Publications. 2012. eBook. Description:

This special collection contains selected papers from the International Conference on Energy and Environmental Protection (ICEEP 2012), held on the 23rd and 24th June, 2012, in Hohhot, China. The 590 peer-reviewed papers cover a wide area and are divided into: Chapter 1: Development and Utilization of Solar Energy; Chapter 2: Development and Utilization of Biomass Energy; Chapter 3: Development and Utilization of Wind Energy; Chapter 4: Nuclear Energy and other Energy Sources; Chapter 5: Energy Storage ... (AN 517227). Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Power Resources / General; Renewable energy sources--Congresses; Environmental protection--Congresses

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

23. Chapter 2 - ISA Server 2006 Client Types and Automating Client Provisioning

In *Dr. Tom Shinder's ISA Server 2006 Migration Guide*, 2007 :47-126
Language: English. DOI: 10.1016/B978-159749199-0/00002-2 Abstract:
Publisher Summary This chapter discusses ISA Server 2006 Client types and automating client provisioning. Computers that go through the ISA server to access resources outside their networks fall into one or more ISA Server 2006 client type categories, which includes the SecureNAT client, the Firewall client, the Web Proxy client. A SecureNAT client is any device configured with a default gateway address that can route Internet-bound connections through the ISA Server 2006 firewall. The primary purpose of the SecureNAT client configuration is to enable non-Microsoft operating systems to access a broader range of protocols than is supported by the Web Proxy client configuration. The ISA Server 2006 Firewall client uses an improved Remote Winsock Proxy Protocol that encrypts the communication channel between the Firewall client and the ISA Server 2006 firewall's Firewall service. The Firewall Client software adopts the centralized settings configured by the ISA Server 2006 computer. The configuring DHCP Servers to Support Web Proxy and Firewall Client Autodiscovery is also elaborated in the chapter. (AN: B9781597491990000022), Database: ScienceDirect



Full Text Finder

USPTO Full Text Options

24. **Google Apps : Mastering Integration and Customization: Scale Your Applications and Projects Onto the Cloud with Google Apps**

By: Morel, Médéric. Birmingham [U.K.] : Packt Publishing, 2011. eBook.

Description: This is a practical hands-on book with clear instructions and lot of code examples. It takes a simple approach, guiding you through different architectural topics using realistic sample projects. A single project is implemented using different architectural styles to make the reader understand the details of each style. There are also many small independent code samples to explain design patterns, WCF, and localization. This book is for people familiar with the ASP.NET framework using either C# or ... (AN 390160), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Data Processing; Application software; **Web** site development--Computer programs

[PDF Full Text](#) [EPUB Full Text](#) [USPTO Full Text Options](#)

[Download](#)

[Table of Contents](#)

[Most Relevant Pages From This eBook](#)

25. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework

By Heartfield, Ryan; Loukas, George. In *Computers & Security*. July 2018 76:101-127 Language: English. DOI: 10.1016/j.cose.2018.02.020 Abstract: The notion that the human user is the weakest link in information security has been strongly, and, we argue, rightly contested in recent years. Here, we take a step further showing that the human user can in fact be the strongest link for detecting attacks that involve deception, such as application masquerading, spearphishing, WiFi evil twin and other types of semantic social engineering. Towards this direction, we have developed a human-as-a-security-sensor framework and a practical implementation in the form of Cogni-Sense, a Microsoft Windows prototype application, designed to allow and encourage users to actively detect and report semantic social engineering attacks against them. Experimental evaluation with 26 users of different profiles running Cogni-Sense on their personal computers for a period of 45 days has shown that human sensors can consistently outperform technical security systems. Making use of a machine learning based approach, we also show that the reliability of each report, and consequently the performance of each human sensor, can be predicted in a meaningful and practical manner. In an organisation that employs a human-as-a-security-sensor implementation, such as Cogni-Sense, an attack is considered to have been detected if at least one user has reported it. In our evaluation, a small organisation consisting only of the 26 participants of the experiment would have exhibited a missed detection rate below 10%, down from 81% if only technical security systems had been used. The results strongly point towards the need to actively involve the user not only in prevention through cyber hygiene and user-centric security design, but also in active cyber threat detection and reporting. (AN: S0167404818301780), Database: ScienceDirect

Subjects: Information Security; Social Engineering; Cyber Crime; Semantic Attacks; Intrusion detection



Full Text Finder

USPTO Full Text Options

26. Handbook of Green Information and Communication Systems

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S.
Amsterdam : Academic Press, 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green Information and Communications Systems. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green information and communication systems are covered from a network ... (AN 485200), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

27. Handbook of Server and Middleware Computing

By: Roundtree, Clarissa; Watt, Elwood. Delhi : Academic Studio, 2012. eBook. Description: Chapter 1 - Introduction to Sedimentology Chapter 2 - Clastic Rock Chapter 3 - Sedimentary Structures Chapter 4 - Aeolian Processes Chapter 5 - Limestone Chapter 6 - Angoumian Chapter 7 - Introduction to Mineralogy Chapter 8 - History of Mineralogy Chapter 9 - Physical Mineralogy (AN 446642), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Client-Server Computing; Middleware; Client/server computing

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

28. Intelligent Transportation Systems

By: Pringle, Drew. Edition: 1st ed. Delhi : Research World. 2012. eBook.
Description: Chapter 1 - Intelligent Transportation System Chapter 2 - Traffic Enforcement Camera Chapter 3 - Intelligent Speed Adaptation Chapter 4 - Vehicle Infrastructure Integration Chapter 5 - Traffic Signal Preemption Chapter 6 - Speed Limit Chapter 7 - National Transportation Communications for Intelligent Transportation System Protocol Chapter 8 - Active Traffic Management and Traffic Camera Chapter 9 - STREAMS Integrated Intelligent Transport System and Urban Traffic Management and Control Chapter 10 ... (AN 396959), Database: eBook Collection (EBSCOhost)

Subjects: BUSINESS & ECONOMICS / Industries / Transportation; TRANSPORTATION / Public Transportation; Intelligent transportation systems

PDF Full Text	USPTO Full Text Options	Download
Table of Contents	Most Relevant Pages From This eBook	

29. Sustainable ICTs and Management Systems for Green Computing

By: Kaabouch, Naima; Hu, Wen Chen. Hershey, PA : IGI Global. 2012. eBook. Description: 'This book focuses on information technology using sustainable green computing to reduce energy and resources used'-- Provided by publisher. (AN 458135), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Electronics / Digital; TECHNOLOGY & ENGINEERING / Electronics / Microelectronics; Electronic data processing departments; Electronic apparatus and appliances-- Environmental aspects; Computer **networks**--Energy conservation; Telecommunication--Energy conservation; Green technology; Electronic data processing--Energy conservation

PDF Full Text	USPTO Full Text Options	Download
Table of Contents	Most Relevant Pages From This eBook	

30. Advances in Enterprise Information Technology Security

By: Herrmann, Francine; Khadraoui, Djamel. Hershey [Pa.] : IGI Global. 2007. eBook. Description: 'This book provides a broad working knowledge of all the major security issues affecting today's enterprise IT activities. Multiple techniques, strategies, and applications are thoroughly examined, presenting the tools to address opportunities in the field. It is an all-in-one reference for IT managers, network administrators, researchers, and students'--Provided by publisher. (AN 185367), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / General; COMPUTERS / Security / Networking; COMPUTERS / Security / Online Safety & Privacy; Computer security; Data protection; Business enterprises--Computer networks--Security measures; Information technology--Security measures

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

[EBSCO Support Site](#) | [Privacy Policy](#) | [Terms of Use](#) | [Copyright](#) | [Contact Us](#)

powered by EBSCOhost

© 2019 EBSCO Industries, Inc. All rights reserved.



1. Handbook of **Systems** Biology : Concepts and Insights

By: Dekker, Job; Vidal, Marc; Walhout, Marian. Edition: 1st ed. Boston : Academic Press. 2013. eBook. Description: This book provides an entry point into **Systems** Biology for researchers in genetics, molecular biology, cell biology, microbiology and biomedical science to understand the key concepts to expanding their work. Chapters organized around broader themes of Organelles and Organisms, **Systems** Properties of Biological Processes, Cellular Networks, and **Systems** Biology and Disease discuss the development of concepts, the current applications, and the future prospects. Emphasis is placed on concepts and insights ... (AN 485494). Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Molecular Biology; **COMPUTERS** / Bioinformatics; MATHEMATICS / Applied; **Systems** biology--Handbooks, manuals, etc; Bioinformatics--Handbooks, manuals, etc

PDF Full Text USPTO Full Text Options Download
Table of Contents Most Relevant Pages From This eBook

2. An Intrusion Detection **System** for Network Security based on an Advanced Honeypots Server.

By: Veena, K.; Meena, K.. *International Journal of Simulation -- Systems, Science & Technology*, Aug2018, Vol. 19 Issue 4, p2.1-2.8, 8p Abstract: The current greatest challenge to Network security is cyber warfare. Every part of **computer** network security is an essential component. In the existing technologies **computer** networks and **systems** are more crucially concerned with network security. The greatest challenge in network is addressing security to the server side. This latest end-to-end research paper recommends to improve the security performance to protect the network from intruders. An advanced honeypot based Intrusion Detection technique is used to detect and analyze threats to ensure security. The Honeypot technique adds a layer to the network security to enhance its performance. A key feature of honeypot is to distract the attacker from the real **system** to derive important information about hacker activities. To validate whether the clients are authorized or unauthorized and monitor the unauthorized client activities, as a first step we use IP validation together with vulnerability detection of user activities. In the second step we use voice recognition as detectors of malicious attacks. Once IP validation and voice recognition are processed and matched then the client is an authorized client and the packet is transmitted to the server, but if not matched it is an unauthorized client, then the packet transmits it to the honeypot server. Our experiment has demonstrated that this particular approach can successfully identify unknown attacks with greater than 95% detection rate and less than 1% false alarm rate. [ABSTRACT FROM AUTHOR]; DOI: 10.5013/IJSSST.a.19.04.02; (AN 133416882), Database: Applied Science & Technology Source

Subjects: Computer security; Computer networks; Computer Systems Design Services; Honeypots (Network security)

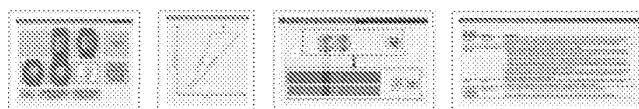
PDF Full Text (629KB) USPTO Full Text Options

3. Offline Management in Virtualized Environments.

By: THORAT, NISHANT; RAGHAVENDRAN, ARVIND; GROVES, NIGEL.
Communications of the ACM, Apr2013, Vol. 56 Issue 4, p75-81, 7p, 4
Diagrams, 2 Charts, 1 Graph Abstract: The article discusses the information
technology (IT) management of combined virtual and physical computing
machines, and mentions topics such as the efficiency of virtualization,
operations management, and IT management tools. **Computer** hardware,
computer network architecture, and IT vendors are discussed, as well as
offline management, antivirus **computer** security, virtual machine patching.
The offline management products Virtual Machine Servicing Tool and
VMware vCenter Protect Essentials Plus are mentioned, as well as data
access systems.; DOI: 10.1145/2436256.2436273; (AN 87497840).
Database: Applied Science & Technology Source

Subjects: Information technology management; **Virtual** machine **systems**;
Computer input-output equipment; **Computer** software industry --
Management; **Computer** architecture; **Computer** security; **Computer** and
peripheral equipment manufacturing; **Computer** Terminal and Other
Computer Peripheral Equipment Manufacturing; Software Publishers;
Computer, **computer** peripheral and pre-packaged software merchant
wholesalers; **Computer** and **Computer** Peripheral Equipment and Software
Merchant Wholesalers; **Computer** and software stores; Software publishers
(except video game publishers); Management

Show all 7 images



PDF Full Text (8MB) USPTO Full Text Options

4. **System cum Program-Wide Lightweight Malicious Program Execution Detection Scheme for Cloud.**

By: Gupta, Sanchika; Kumar, Padam. *Information Security Journal: A Global Perspective*. 2014, Vol. 23 Issue 3, p86-99. 14p. Abstract: Cloud is prone to a set of well-known network and host-based attacks from cloud insiders, cloud users, and outside attackers. This paper concretely focuses over the detection of malware and program modification-based attacks through identification of malicious program executions and malware at the client virtual machines and hosts in a cloud environment. The paper also focuses on the related techniques for malware detection using system call sequence measures. An immediate system call structure-based program cum system-wide technique is proposed for the detection of anomalous program executions and malwares in the cloud. The algorithm is validated over University of New Mexico sendmail data set. Effective deployment architecture for such an implementation is also presented as a distributed cum centralized intrusion prevention system (IPS). The proposed IPS also solves the problem of individual IPS getting malformed at client virtual machine with the use of both process and system level based detection strategies. The paper provides detailed results and experimentations of the proposed intrusion detection technique on a private cloud with open nebula and virtual box. [ABSTRACT FROM AUTHOR] DOI: 10.1080/19393555.2014.942017. (AN: 99462734), Database: Computer Source

Subjects: CLOUD computing; WEB hosting; CYBERTERRORISM; MALWARE; NEBULA (Computer program language)

[HTML Full Text](#) [PDF Full Text](#) (530KB)

[USPTO Full Text Options](#)

5. Data Division and Replication Approach for Improving Security and Availability of Cloud Storage

In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) Computing Communication Control and Automation (ICCUBEA), 2018 Fourth International Conference on. :1-4 Aug. 2018; IEEE Language: English. Abstract: Large, distributed network **systems** such as the Cloud cater to the immense data storage needs of people around the world. This data stored upon the cloud may be sensitive, which makes the Security aspect of these Cloud **systems** extremely imperative. The Cloud nodes **host** this data. If these nodes are compromised by a malicious entity then consequences may be dire. In this paper we have proposed and put forth the results of a **system** which will implement a storage methodology that uses the Division and Replication strategy for storing the data. In this **system**, the file will be fragmented and these fragments will be replicated according to the replication factor before storing it upon the cloud. The fragments are dispersed such that consecutive nodes on the Cloud do not hold the fragments of a same file and so that even if a node is compromised no significant information is leaked to the attacker. This **system** will enhance cloud security using Division and Replication of data in Cloud for Optimal Performance and Security (DROPS) methodology. This additional security will come without any cryptographic techniques being applied. Lack of these computation heavy cryptographic techniques will mean that security will come without the compromise of increasing the computation load. The **system** will analyze the performance of our methodology by portraying it in a virtual environment **comprising** of virtual machines which form a Cloud network. We will depict the results of our **system** and how it handled storing data onto the cloud. (AN: *edsee.8697355*), Database: IEEE Xplore Digital Library

Subjects: Communication, Networking and Broadcast Technologies; Components, Circuits, Devices and **Systems**; Computing and Processing; Robotics and Control **Systems**; Signal Processing and Analysis; Cloud computing; Cryptography; **Virtual** machining; Databases; **Computer** security; Image color analysis; Availability; Cloud; Data Fragments; Redundancy; Replication; Security; T – coloring

Get Full Text at **IEEE Xplore®**

USPTO Full Text Options

6. Encyclopedia of the Solar System

By: Spohn, T.; Breuer, Doris; Johnson, T. V. Edition: Third edition.
Amsterdam : Elsevier. 2014. eBook. Description: The Encyclopedia of the Solar System, Third Edition—winner of the 2015 PROSE Award in Cosmology & Astronomy from the Association of American Publishers—provides a framework for understanding the origin and evolution of the solar system, historical discoveries, and details about planetary bodies and how they interact—with an astounding breadth of content and breathtaking visual impact. The encyclopedia includes the latest explorations and observations, hundreds of color digital images and illustrations, ... (AN 596600), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Space Science

[PDF Full Text](#) [EPUB Full Text](#) [USPTO Full Text Options](#)

[Download](#)

[Table of Contents](#)

[Most Relevant Pages From This eBook](#)

7. Embedded System Design

By: Marwedel, Peter. New York : Springer. 2006. eBook. Description: Until the late eighties, information processing was associated with large mainframe computers and huge tape drives. During the nineties, this trend shifted towards information processing with personal computers, or PCs. The trend towards miniaturization continues. In the future, most of the information processing systems will be quite small and embedded into larger products such as transportation and fabrication equipment. Hence, these kinds of systems are called embedded systems. It is expected ... (AN 118359), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Electronics / Circuits / General; **COMPUTERS** / CAD-CAM; **COMPUTERS** / Computer Science; TECHNOLOGY & ENGINEERING / Electrical; Embedded computer systems--Design

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#)

[Most Relevant Pages From This eBook](#)

8. **Garbage Collection for Virtual Memory Computer Systems.**

By: Randell, B.; Baecker, H. D.. *Communications of the ACM*, Nov72, Vol. 15 Issue 11, p981-986, 6p, 3 Charts Abstract: In list processing there is typically a growing demand for space during program execution. This paper examines the practical implications of this growth within a **virtual memory computer system**, proposes two new garbage collection techniques for **virtual memory systems**, and compares them with traditional methods by discussion and by simulation. [ABSTRACT FROM AUTHOR]; (AN 5263794), Database: Applied Science & Technology Source

Subjects: Garbage collection (**Computer science**); **Computer** programming; Memory management (**Computer science**); **Computer** algorithms; **Virtual** storage (**Computer science**); List processing (Electronic **computers**); **Computer systems** design and related services (except video game design and development); Custom **Computer** Programming Services; Other **Computer** Related Services

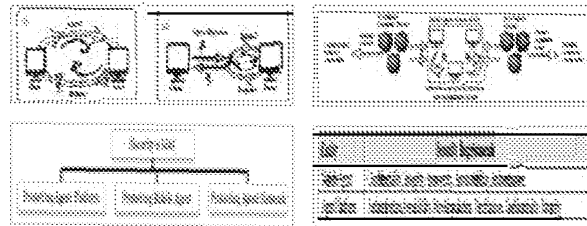
[PDF Full Text \(509KB\)](#) [USPTO Full Text Options](#)

9. **Mobile Agents System Security: A Systematic Survey.**

By: BAGGA, PALLAVI; HANS, RAHUL. *ACM Computing Surveys*, Nov2017, Vol. 50 Issue 5, p65:1-65:45, 45p, 6 Diagrams, 14 Charts, 2 Graphs Abstract: A pivotal cause for the boom of Mobile Agent paradigm relies on the competence to ward off security attacks. This article surveys the prevalent attacks on the mobile agents and the agent platforms; the existing countermeasures and their curbs, catering threefold benefaction: First, to acquaint the researchers with numerous security requirements and the objectives. Second, to analyze the different detection and prevention mechanisms mitigating the security bottlenecks in Mobile Agents **System**. Third, to address the future security challenges. In a nutshell, this survey hands over a key to researchers who primarily target the security concerns of the mobile agent-based applications. [ABSTRACT FROM AUTHOR]; DOI: 10.1145/3095797; (AN 125367039), Database: Applied Science & Technology Source

Subjects: User-centered **system** design; Cyberterrorism; Mobile agent **systems**; **Computer** security; **System** analysis

Show all 26 images



PDF Full Text (11.1MB) USPTO Full Text Options

10. Why build a **virtual brain**? Large-scale neural simulations as jump start for cognitive computing.

By: Colombo, Matteo. *Journal of Experimental & Theoretical Artificial Intelligence*. Apr2017, Vol. 29 Issue 2, p361-370. 10p. Abstract: Despite the impressive amount of financial resources recently invested in carrying out large-scale brain simulations, it is controversial what the pay-offs are of pursuing this project. One idea is that from designing, building, and running a large-scale neural simulation, scientists acquire knowledge about the computational performance of the simulating **system**, rather than about the neurobiological **system** represented in the simulation. It has been claimed that this knowledge may usher in a new era of neuromorphic, cognitive computing **systems**. This study elucidates this claim and argues that the main challenge this era is facing is not the lack of biological realism. The challenge lies in identifying general neurocomputational principles for the design of artificial **systems**, which could display the robust flexibility characteristic of biological intelligence. [ABSTRACT FROM AUTHOR] DOI: 10.1080/0952813X.2016.1148076. (AN: 120687120), Database: Computer Source

Subjects: MEDICAL simulation; BRAIN research; NEURAL conduction; SIMULATION methods & models; REALISM

[HTML Full Text](#) [PDF Full Text](#) (583KB)

[USPTO Full Text Options](#)

11. Distributed Network **Systems** : From Concepts to Implementations

By: Jia, Weijia; Zhou, Wanlei. Series: Network Theory and Applications, v. 15. New York : Springer. 2005. eBook. Description: This textbook covers both theoretical and practical aspects of distributed computing. It describes the client-server model for developing distributed network **systems**, the communication paradigms used in a distributed network **system**, and the principles of reliability and security in the design of distributed network **systems**. Based on theoretical introductions, the book presents various implementation strategies and techniques for building distributed network **systems**, including examples in TCP/IP communications, ... (AN 130165). Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Data Transmission **Systems** / General; **COMPUTERS** / Networking / Vendor Specific; **Computer networks**; Electronic data processing--Distributed processing

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

12. Sustainable ICTs and Management **Systems** for Green Computing

By: Kaabouch, Naima; Hu, Wen Chen. Hershey, PA : IGI Global. 2012. eBook. Description: 'This book focuses on information technology using sustainable green computing to reduce energy and resources used'-- Provided by publisher. (AN 458135), Database: eBook Collection (EBSCOhost)

Subjects: **TECHNOLOGY & ENGINEERING** / Electronics / Digital; **TECHNOLOGY & ENGINEERING** / Electronics / Microelectronics; Electronic data processing departments; Electronic apparatus and appliances--Environmental aspects; **Computer networks**--Energy conservation; Telecommunication--Energy conservation; Green technology; Electronic data processing--Energy conservation

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

13. **SYSTEM AND METHOD FOR PROVIDING
COMPUTER SERVICES**

By: Mays, Stephen Mark; Lovullo, JR., Joseph Anthony; Cai, Sandeep.

Patent Application: 13/261133. Filed: September 10, 2008. Published: June 14, 2012. , Database: USPTO Patent Applications

Abstract: A **computer system** and method for providing **computer services** to a user, comprising: a **virtual computer system** comprising at least one **virtual computer** that is created within the **virtual computer system**; a virtualization layer enabling the at least one **virtual computer** to utilize CPU, RAM and storage of a **host computer** within the **virtual computer system**; a **virtual computer selector** providing for the selection of the at least one **virtual computer** on an unscheduled basis; a **storage system**; and a **streaming video content system** for separating streaming video data into a graphical user interface component that contains data display information required by said terminal device in order to locate and draw a user interface and a video stream component that is displayed on a screen of the terminal device within the user interface.

AN: edsPap.20120150992

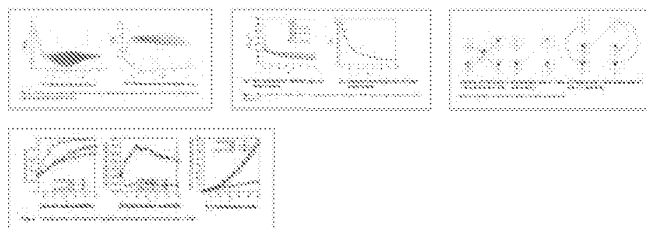
USPTO Full Text Options

14. A novel robust on-line protocol for load-balancing in structured peer-to-peer systems.

By: Tsatsanifos, George; Samoladas, Vasilis. *Computing*. Sep2012, Vol. 94 Issue 8-10, p731-762. 32p. 1 Diagram, 10 Graphs. Abstract: In this paper, we revisit the problem of load-balancing structured peer-to-peer systems with on-line protocols. Load-balancing is of major significance for large-scale decentralized networks in terms of enhanced scalability and performance. The main incentives behind balancing schemes are under-utilization of bandwidth and **computer** resources. Therefore, our methods focus mainly on task-skew. Specifically, we address the problem with on-line protocols on the basis of migration and enhanced availability. In particular, the cornerstones of our methods are the notions of **virtual** nodes, replication and Multiple realities, combined altogether with allocation techniques based on balls-in-bins games. The rationale of our dynamic protocol to depend exclusively on peer load distribution preserves intact the structural properties and search efficiency of the overlay used as an indexing infrastructure, while preserving the semantic information of the data (e.g., range partitioned network). We also propose an effective load-aware mechanism to facilitate robust operations that counteract against contingent churn failures. Finally, our work is complemented with extensive experiments using both real and synthetic data sets. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s00607-012-0199-7. (AN: 79341424), Database: Computer Source

Subjects: **COMPUTER** network protocols; **ROBUST** control; **LOAD** balancing (**Computer** networks); **PEER**-to-peer architecture (**Computer** networks); **COMPUTER** networks; **SCALABILITY** (**Systems** engineering); **DISTRIBUTED** computing; **QUERYING** (**Computer** science); **DATA** replication

Show all 11 images



PDF Full Text (910KB) USPTO Full Text Options

15. **Multiagent Systems : A Modern Approach to Distributed Artificial Intelligence**

By: Weiss, Gerhard. Cambridge, Mass : The MIT Press. 1999. eBook.

Description: This is the first comprehensive introduction to multiagent systems and contemporary distributed artificial intelligence that is suitable as a textbook. The book provides detailed coverage of basic topics as well as several closely related ones. Unlike traditional textbooks, the book brings together many leading experts, guaranteeing a broad and diverse base of knowledge and expertise. It emphasizes aspects of both theory and application, and provides many illustrations and examples. Also included ... (AN 9368), Database: eBook Collection (EBSCOhost)

Subjects: **COMPUTERS** / Intelligence (AI) & Semantics; Intelligent agents (**Computer software**); Distributed artificial intelligence

[PDF Full Text](#) [USPTO Full Text Options](#) [Download](#)

[Table of Contents](#) [Most Relevant Pages From This eBook](#)

16. Multi-objective Swarm Intelligence schedulers for online scientific Clouds.

By: Pacini, Elina; Mateos, Cristian; Garino, Carlos. *Computing*. May2016, Vol. 98 Issue 5, p495-522. 28p. Abstract: Cloud Computing is a promising paradigm for parallel computing. However, as Cloud-based services become more dynamic, resource provisioning in Clouds becomes more challenging. The paradigm, with its promise of virtually infinite resources, seems to suit well in solving resource greedy scientific computing problems. In a Cloud, an appropriate number of **Virtual Machines (VM)** is created and allocated in physical resources for executing jobs. This work focuses on the Infrastructure as a Service (IaaS) model where custom VMs are launched in appropriate **hosts** available in a Cloud to execute scientific experiments coming from multiple users. Finding optimal solutions to allocate VMs to physical resources is an NP-complete problem, and therefore many heuristics have been developed. In this work, we describe and evaluate two Cloud schedulers based on Swarm Intelligence (SI) techniques, particularly Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO). The main performance metrics to study are the number of serviced users by the Cloud and the total number of created VMs in online (non-batch) scheduling scenarios. We also perform a sensitivity analysis by varying the specific-parameter values of each algorithm to evaluate the impact on the performance of the two objective metrics. The intra-Cloud network traffic is also measured. Simulated experiments performed using CloudSim and job data from real scientific problems show that the use of SI-based techniques succeeds in balancing the studied metrics compared to Genetic Algorithms. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s00v07-014-0412-y. (AN: 114679359), Database: Computer Source

Subjects: SWARM intelligence; **COMPUTER** scheduling; CLOUD computing; **VIRTUAL** machine **systems**; **COMPUTER** simulation

[PDF Full Text \(1.2MB\)](#) [USPTO Full Text Options](#)

17. Review on Smart Hospital Management **System** Technologies

By: Lakhoua, Najeh. In: Research and Science Today, Vol. 17, pp. 187-204 (AN: edshol.hein.journals.rescito17.17), Database: HeinOnline

Subjects: General



Full Text Finder

USPTO Full Text Options

18. A conceptual framework of information **systems** for organizational creativity support. lessons from empirical investigations.

By: Olszak, Celina M.; Kisielnicki, Jerzy. *Information **Systems** Management*. 2018, Vol. 35 Issue 1, p29-48. 20p. 2 Diagrams, 5 Charts. Abstract: Based on a review of the subject literature, a conceptual framework of information **systems** for organizational creativity support is proposed. The most important elements in creating such a **system** are identified and described. Finally, the results of a survey conducted in twenty-five organizations are used to better understand the most important elements and factors determining the development of information **systems** for organizational creativity support. [ABSTRACT FROM AUTHOR] DOI: 10.1080/10580530.2017.1416945. (AN: 127365748), Database: Computer Source

Subjects: INFORMATION storage & retrieval **systems**; INFORMATION science; EMPIRICAL research; CREATIVE ability; ORGANIZATIONAL change

Show all 7 images



HTML Full Text PDF Full Text (1.8MB) USPTO Full Text Options

19. **Handbook of Green Information and Communication Systems**

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S.
Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green Information and Communications **Systems**. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green information and communication **systems** are covered from a network ... (AN 485200), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

PDF Full Text USPTO Full Text Options Download
Table of Contents Most Relevant Pages From This eBook

20. **Researchers Submit Patent Application, 'System For Virtual Patching Security Vulnerabilities In Software Containers', for Approval (USPTO 20190005246)**

In: Computer Weekly News. Jan 23, 2019, 6226; NewsRX LLC Language: English. Abstract: 2019 JAN 23 (VerticalNews) -- By a News Reporter-Staff News Editor at Computer Weekly News -- From Washington, D.C., VerticalNews journalists report that a patent application by the inventors Cherny, [...] (AN: edsgcl.575442488), Database: General OneFile

Subjects: Product enhancement; **Systems**/data security software; Containers -- Product enhancement; Containers -- Intellectual property; **Systems** and data security software -- Product enhancement; **Systems** and data security software -- Intellectual property

 Full Text Finder USPTO Full Text Options

21. Brokerage-based dependability integration in cloud computing services.

By: Abderrahim, Wiem; Choukair, Zied. *Journal of Supercomputing*, Jul2018, Vol. 74 Issue 7, p3359-3387, 29p Abstract: Cloud computing plays a significant role to store and analyze the exponentially growing volume of generated data. However, cloud computing is inherently a frequent environment for failures and its services undergo long downtime periods. These failures threaten the user experience especially when we take into consideration that not only the currently generated data have a tremendous volume but also it presents new types and different generation velocities. Therefore, the aim of this paper is to propose a broker architecture, which ensures that behavioral requirements in terms of dependability properties are met by the provided cloud service at the infrastructure, platform and service levels. This architecture takes the decision to continue the service delivery with the same cloud provider or to migrate toward a new provider based on the evaluation of the fault severity impact. DBA takes into consideration the interdependence between the cloud service models and formalizes all dependability attributes with a single state-based stochastic model. Results demonstrate the introduced amelioration in terms of dependability properties compared to classic cloud service delivery. The main contribution concerns safety improvement by avoiding catastrophic failures. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11227-018-2388-4; (AN 130553727), Database: Applied Science & Technology Source

Subjects: Cloud computing; Software as a service; **Computer system** failures; Distributed computing; **Computer** architecture; Reliability (Engineering); Data Processing, Hosting, and Related Services

[HTML Full Text](#) [PDF Full Text \(2MB\)](#) [USPTO Full Text Options](#)

22. Bi-objective decision support **system** for task-scheduling based on genetic algorithm in cloud computing.

By: Aziza, Hatem; Krichen, Saoussen. *Computing*. Feb2018, Vol. 100 Issue 2, p65-91. 27p. Abstract: We address in this paper the task-scheduling in cloud computing. This problem is known to be NP<inline-graphic></inline-graphic>-hard due to its combinatorial aspect. The main role of our model is to estimate the time needed to run a set of tasks in cloud and in turn reduces the processing cost. We propose a genetic approach for modelling and optimizing a task-scheduling problem in cloud computing. The experimental results demonstrate that our solution successfully competes with previous task-scheduling algorithms. For this, we develop a decision support **system** based on the core of CloudSim. In terms of processing cost, the obtained results show that our approach outperforms previous scheduling methods by a significant margin. In terms of makespan, the obtained schedules are also shorter than those of other algorithms. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s00607-017-0566-5. (AN: 128228124), Database: Computer Source

Subjects: CLOUD computing; DECISION support **systems**; GENETIC algorithms; PRODUCTION scheduling; COMBINATORIAL analysis

[HTML Full Text](#) [PDF Full Text \(2.3MB\)](#) [USPTO Full Text Options](#)

23. Patent Issued for **System** And Method For Deploying An Application In A **Computer System** (USPTO 10,205,771)

In: **Computer Weekly News**. Feb 27, 2019, 2034; NewsRX LLC Language: English. Abstract: 2019 FEB 27 (VerticalNews) -- By a News Reporter-Staff News Editor at **Computer Weekly News** -- According to news reporting originating from Alexandria, Virginia, by VerticalNews journalists, a patent by [...] (AN: edsgcl.576599380), Database: General OneFile

Subjects: United States; VMware Inc. -- Intellectual property; **Computer** software industry -- Intellectual property; **Computer** software industry -- Methods

 [Full Text Finder](#) [USPTO Full Text Options](#)

24. Patent Issued for Method And Apparatus For
Hosting A Multitasking Guest On A **Host System**
(USPTO 10,095,544)

In: Journal of Engineering. Oct 22, 2018, 957; NewsRX LLC Language: English. Abstract: 2018 OCT 22 (VerticalNews) -- By a News Reporter-Staff News Editor at Journal of Engineering -- From Alexandria, Virginia, VerticalNews journalists report that a patent by the inventors Evripidou, Christos [...] (AN: edsgcl.559081875), Database: Academic OneFile

Subjects: Germany; Software quality; Patent/copyright issue; Robert Bosch GmbH -- Intellectual property; Robert Bosch GrnbH -- Reports; **Virtual computer systems** -- Methods; **Virtual computer systems** -- Reports; Software -- Methods; Software -- Reports; Patents -- Methods; Patents -- Reports; Periodical publishing -- Intellectual property; Periodical publishing -- Methods; Periodical publishing -- Reports; **Computer science** -- Methods; **Computer science** -- Reports



Full Text Finder

USPTO Full Text Options

25. 'Management Of Authenticator Information In A
Computer System' in Patent Application Approval
Process (USPTO 20180234400)

In: Computer Weekly News. Sept 5, 2018, 1153; NewsRX LLC Language: English. Abstract: 2018 SEP 5 (VerticalNews) -- By a News Reporter-Staff News Editor at Computer Weekly News -- A patent application by the inventors Mononen, Tero (Helsinki, FI); Rossi, Markku (Helsinki, FI); [...] (AN: edsgcl.552671932), Database: General OneFile

Subjects: Finland; Company business management; Patent/copyright issue; Patents



Full Text Finder

USPTO Full Text Options

26. Patent Issued for Automatically Reconfiguring Physical Switches To Be In Synchronization With Changes Made To Associated **Virtual System** (USPTO 10,033,584)

In: Information Technology Newsweekly. August 7, 2018, 3737; NewsRX LLC Language: English. Abstract: 2018 AUG 7 (VerticalNews) -- By a News Reporter-Staff News Editor at Information Technology Newsweekly -- According to news reporting originating from Alexandria, Virginia, by VerticalNews journalists, a patent by [...] (AN: edsgcl.548993646), Database: General OneFile

Subjects: United States; California; Patent/copyright issue; Juniper Networks Inc. -- Intellectual property; **Computer peripherals industry** -- Intellectual property; **Virtual computer systems**; Patents



Full Text Finder

USPTO Full Text Options

27. Researchers Submit Patent Application, 'Processing Method Of Data Redundancy And **Computer System** Thereof', for Approval (USPTO 20190155772)

In: Information Technology Newsweekly. June 11, 2019, 7776; NewsRX LLC Language: English. Abstract: 2019 JUN 11 (VerticalNews) -- By a News Reporter-Staff News Editor at Information Technology Newsweekly -- From Washington, D.C., VerticalNews journalists report that a patent application by the inventors Yu, [...] (AN: edsgcl.588229186), Database: General OneFile

Subjects: Taiwan; Company personnel management



Full Text Finder

USPTO Full Text Options

28. **Patent Application Titled 'Computer System Management Method And Computer System' Published Online (USPTO 20180246763)**

In: Information Technology Newsweekly. Sept 18, 2018, 2208; NewsRX LLC
Language: English. Abstract: 2018 SEP 18 (VerticalNews) -- By a News
Reporter-Staff News Editor at Information Technology Newsweekly --
According to news reporting originating from Washington, D.C., by
VerticalNews journalists, a patent application [...] (AN: edsgcl.554412217),
Database: General OneFile

Subjects: Japan; Company business management; Patent/copyright issue;
Patents -- Methods

 [Full Text Finder](#) [USPTO Full Text Options](#)

29. **Patent Issued for System And Method For Providing Data And Application Continuity In A Computer System (USPTO 10,110,667)**

In: Journal of Engineering. Nov 5, 2018, 6616; NewsRX LLC Language:
English. Abstract: 2018 NOV 5 (VerticalNews) -- By a News Reporter-Staff
News Editor at Journal of Engineering -- Geminare Inc. (Toronto, Canada)
has been issued patent number 10,110,667, according to news reporting [...] (AN: edsgcl.561038457), Database: Academic OneFile

Subjects: Patent/copyright issue; Periodical publishing -- Intellectual
property; Periodical publishing -- Methods; Patents -- Methods

 [Full Text Finder](#) [USPTO Full Text Options](#)

30. Security in Internet of Things: issues, challenges, taxonomy, and architecture.

By: Adat, Vipindev; Gupta, B. B.. *Telecommunication Systems*, Mar2018, Vol. 67 Issue 3, p423-441, 19p Abstract: Internet technology is very pervasive today. The number of devices connected to the Internet, those with a digital identity, is increasing day by day. With the developments in the technology, Internet of Things (IoT) become important part of human life. However, it is not well defined and secure. Now, various security issues are considered as major problem for a full-fledged IoT environment. There exists a lot of security challenges with the proposed architectures and the technologies which make the backbone of the Internet of Things. Some efficient and promising security mechanisms have been developed to secure the IoT environment, however, there is a lot to do. The challenges are ever increasing and the solutions have to be ever improving. Therefore, aim of this paper is to discuss the history, background, statistics of IoT and security based analysis of IoT architecture. In addition, we will provide taxonomy of security challenges in IoT environment and taxonomy of various defense mechanisms. We conclude our paper discussing various research challenges that still exist in the literature, which provides better understanding of the problem, current solution space, and future research directions to defend IoT against different attacks. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11235-017-0345-9; (AN 128110400), Database: Applied Science & Technology Source

Subjects: Internet of things; **Computer** architecture; **Computer** security; Denial of service attacks; Intrusion detection **systems** (**Computer** security)

[HTML Full Text](#) [PDF Full Text](#) (1.6MB) [USPTO Full Text Options](#)

[EBSCO Support Site](#) | [Privacy Policy](#) | [Terms of Use](#) | [Copyright](#) | [Contact Us](#)

powered by EBSCOhost

© 2019 EBSCO Industries, Inc. All rights reserved.

DOCKET NO.: LCOM_ISO_US02
Application No.: 15/910,734
Office Action Dated: July 25, 2019

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
L3 Technologies, Inc.

Confirmation No.: 2365

Application No.: 15/910,734

Group Art Unit: 2498

Filing Date: March 2, 2018

Examiner: Truong, Thanhnga B.

For: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

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

Sir:

REPLY PURSUANT TO 37 CFR § 1.111

In response to the Official Action dated **July 25, 2019**, reconsideration is respectfully requested in view of the amendments and/or remarks as indicated below:

- ☐ **Amendments to the Specification** begin on page N/A of this paper.
- ☐ **Amendments to the Claims** are reflected in the listing of the claims which begins on page N/A of this paper.
- ☐ **Amendments to the Drawings** begin on page N/A of this paper and include an attached replacement sheet.
- ☒ **Remarks** begin on page 2 of this paper.
- ☒ The Commissioner is hereby authorized to charge any fee deficiency, charge any additional fees, or credit any overpayment of fees, associated with this application in connection with this filing, or any future filing, submitted to the U.S. Patent and Trademark Office during the pendency of this application, to Deposit Account No. 50-5519.

Doc Code: DISQ.E.FILE

Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15910734

Filing Date: 02-Mar-2018

Applicant/Patent under Reexamination: Hoy

Electronic Terminal Disclaimer filed on August 30, 2019

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed		PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce	
Electronic Petition Request	TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT		
Application Number	15910734		
Filing Date	02-Mar-2018		
First Named Inventor	Robert Hoy		
Attorney Docket Number	LCOM_ISO_US02		
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS		
☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action ☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.			
Owner		Percent Interest	
L3 Technologies, Inc.		100 %	
The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s) 9942198 as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns. In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later: - expires for failure to pay a maintenance fee; - is held unenforceable; - is found invalid by a court of competent jurisdiction; - is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321; - has all claims canceled by a reexamination certificate; - is reissued; or - is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer. ☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.			

☐ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ☐ Small Entity ☐ Micro Entity ☒ Regular Undiscounted	
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ☒ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number <u>77970</u> ☐ A sole inventor ☐ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ☐ A joint inventor; all of whom are signing this request	
Signature	/Ryan A. Peddle/
Name	Ryan A. Peddle

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
 Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Acknowledgement Receipt

EFS ID:	37027301
Application Number:	15910734
International Application Number:	
Confirmation Number:	2365
Title of Invention:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS
First Named Inventor/Applicant Name:	Robert B. Hoy
Customer Number:	158266
Filer:	Ryan A. Peddle/Melissa Inzaris
Filer Authorized By:	Ryan A. Peddle
Attorney Docket Number:	LCOM_ISO_US02
Receipt Date:	30-AUG-2019
Filing Date:	02-MAR-2018
Time Stamp:	11:00:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		LCOM_ISO_US02_AS_FILED_Reply_to_NFOA.pdf	109662	yes	2
			3080775be73ac4387655b871bc3e38df6ec904bf		

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Applicant Arguments/Remarks Made in an Amendment	2	2
Warnings:			
Information:			
Total Files Size (in bytes):			109662
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.			

Electronic Acknowledgement Receipt

EFS ID:	37027257
Application Number:	15910734
International Application Number:	
Confirmation Number:	2365
Title of Invention:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS
First Named Inventor/Applicant Name:	Robert B. Hoy
Customer Number:	158266
Filer:	Ryan A. Peddle/Melissa Inzaris
Filer Authorized By:	Ryan A. Peddle
Attorney Docket Number:	LCOM_ISO_US02
Receipt Date:	30-AUG-2019
Filing Date:	02-MAR-2018
Time Stamp:	10:58:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 160
RAM confirmation Number	E20198TA58334955
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	33441	no	2
			7740ad9eb138b727da80d73c2613b669acdb10f4		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30458	no	2
			7bb06829bb2de4237ca8700e26488cfb6da15ded		
Warnings:					
Information:					
Total Files Size (in bytes):			63899		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

REMARKS

Claims 28-47 of the present application are pending. No claims have been amended herein. No claims have been added or canceled herein. No new matter has been added.

Double Patenting Rejection

Claims 28-47 stand rejected under the judicially created doctrine of non-statutory obviousness-type double patenting as allegedly being unpatentable over claims 1-23 of U.S. Patent No. 9,942,198. As a proper terminal disclaimer is being filed herewith, the double patenting rejection is moot and withdrawal thereof is respectfully requested.

CONCLUSION

Insofar as the Office Action's rejections having been adequately addressed, it is believed that the present application is in condition for allowance and such action is respectfully requested.

Date: August 30, 2019

Ryan A. Peddle/
Ryan A. Peddle
Registration No. 77,970

Condo Roccia Koptiw LLP
1800 JFK Blvd., Suite 1700
Philadelphia, PA 19103
Telephone: (215) 558-5740
Facsimile: (215) 558-5676

Electronic Patent Application Fee Transmittal

Application Number:	15910734			
Filing Date:	02-Mar-2018			
Title of Invention:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS			
First Named Inventor/Applicant Name:	Robert B. Hoy			
Filer:	Ryan A. Peddle/Melissa Inzaris			
Attorney Docket Number:	LCOM_ISO_US02			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				160

<i>Index of Claims</i> 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant						☐ CPA		☒ T.D.		☐ R.1.47
CLAIM		DATE								
Final	Original	04/30/2018	03/15/2019	07/22/2019	11/07/2019					
	1	-	-	-						
	2	-	-	-						
	3	-	-	-						
	4	-	-	-						
	5	-	-	-						
	6	-	-	-						
	7	-	-	-						
	8	-	-	-						
	9	-	-	-						
	10	-	-	-						
	11	-	-	-						
	12	-	-	-						
	13	-	-	-						
	14	-	-	-						
	15	-	-	-						
	16	-	-	-						
	17	-	-	-						
	18	-	-	-						
	19	-	-	-						
	20	-	-	-						
	21	-	-	-						
	22	-	-	-						
	23	-	-	-						
	24	-	-	-						
	25	-	-	-						
	26	-	-	-						
	27	-	-	-						
1	28	✓	✓	✓	=					
2	29	✓	✓	✓	=					
3	30	✓	✓	✓	=					
4	31	✓	✓	✓	=					
5	32	✓	✓	✓	=					
6	33	✓	✓	✓	=					
7	34	✓	✓	✓	=					
8	35	✓	✓	✓	=					
9	36	✓	✓	✓	=					
10	37	✓	✓	✓	=					
11	38	✓	✓	✓	=					
12	39	✓	✓	✓	=					
13	40	✓	✓	✓	=					
14	41	✓	✓	✓	=					
15	42	✓	✓	✓	=					

<i>Index of Claims</i> 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

CLAIM		DATE									
Final	Original	04/30/2018	03/15/2019	07/22/2019	11/07/2019						
16	43	✓	✓	✓	=						
17	44	✓	✓	✓	=						
18	45	✓	✓	✓	=						
19	46	✓	✓	✓	=						
20	47	✓	✓	✓	=						

Issue Classification 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

CPC						
Symbol				Type	Version	
H04L	/	63	/	0272	F	2013-01-01
G06F	/	21	/	53	I	2013-01-01
H04L	/	63	/	101	I	2013-01-01
G06F	/	9	/	45558	I	2013-01-01
G06F	/	2009	/	45587	A	2013-01-01

CPC Combination Sets							
Symbol				Type	Set	Ranking	Version
	/		/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498	07 November 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	28	1

U.S. Patent and Trademark Office

Part of Paper No.: 20191107

Issue Classification 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04L	/	63	/ 0272

NON-CLAIMED			
	/		/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498	07 November 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	28	1

Issue Classification 	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination Hoy et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

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

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

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 20	
/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498 (Primary Examiner) _____ (Date) _____		07 November 2019 (Date)	O.G. Print Claim(s) 28
			O.G. Print Figure 1

U.S. Patent and Trademark Office

Part of Paper No.: 20191107



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

158266 7590 11/08/2019
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2498	

DATE MAILED: 11/08/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/910,734	03/02/2018	Robert B. Hoy	LCOM_ISO_US02	2365

TITLE OF INVENTION: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1000	\$0.00	\$0.00	\$1000	02/10/2020

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: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.