Amendments to the Specification:

Amendments to the specification are indicated below, wherein new text is underlined and deleted text is indicated either by strikethrough font or within double brackets.

Please amend the following paragraph on page 1 of the specification following the TITLE:

CROSS REFERENCE TO RELATED APPLICATIONS

This application ~~claims the benefit of~~ is a continuation of U.S. Patent Application No. 13/981,896, filed July 29, 2013, which is a National Stage Entry under 35 U.S.C. § 371 of Patent Cooperation Treaty Application No. PCT/US2012/023027, filed January 27, 2012, which claims priority from U.S. Provisional Application ~~serial number~~ No. 61/436,932, filed January 27, 2011, which [[is]] are herein incorporated by reference in [[its]] their entirety.

Ex.1002
CISCO SYSTEMS, INC. / Page 1 of 517

INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

Related applications

This application claims the benefit of U.S. provisional application serial number 61/436,932 filed on January 27, 2011, which is herein incorporated by reference in its entirety.

Field of Invention

This invention relates to the protection of computer systems from injurious software that can be encountered while browsing or accessing the Internet, and also to the protection of local Internet networks (LANS) that have access to the Internet.

Description of the Prior Art

The Internet provides access to a large number of computer systems from which beneficial or harmful data may be retrieved by a computer attached to and communicating over the Internet. Harmful data that can be accessed through the Internet includes a variety of viral software constructs, generally referred to as malicious software or malware. Malware normally is downloaded to a computer completely unintentionally and without the knowledge of the individual computer user.

The results of an infection of the computer system are possible malfunctions or inefficiency. In addition, there are possible security losses, such as the loss of all data that is accessible to that computer system and the installation of various types of subservient software on the infected system that allows for the control of Internet operations or other activities of the computer from a remote location unknown by the user.

One typical way that such malware is delivered to an uninfected computer system is that the user of the system accesses a website through an Internet browser such as Internet Explorer or Firefox, or any of a variety of other well-known programs configured for browsing on the Internet, and receives from that

website a data packet that contains malicious code. This malicious code may be automatically downloaded to a user's computer through a webpage, the website URL of which may have been emailed to the user, or the user may have purposely accessed the website because the user is familiar with it. In either case, the website has secretly been hacked to carry the malicious code in its HTML coding. The hacked webpage has code that redirects the user to a mothership server hosting the real exploit. If the exploit is successful due to a vulnerability, etc., a toolset is then silently installed on the user's computer, with results that will be described below.

Another typical exploit that is used to attempt to introduce malicious software to a system is via an attachment (typically a PDF) that is either received or downloaded from a website. When opened, the attachment starts a hidden stub code that exploits a vulnerability in, for example, the application Adobe Reader where the attack is via a PDF exploit. The stub code is a small piece of code that when opened by the browser initiates on the host computer a software operation that listens to a specified remote Internet server via a port of the host computer. The port is usually port 80 or Port 443, both of which are normally universally allowed ports on ordinary computer systems through which the Internet can be accessed. The stub code program downloads a secondary payload software module, commonly an .exe file, from the remote Internet server. This secondary payload is loaded into the host computer, which is at this point infected. The secondary payload file then executes and starts performing various functions according to a toolset.

The toolsets of either exploit technique comprise software that may do any of the following functions:

i. the toolset performs and reports a recon of the system to assess what is available there as a resource and the files, etc., stored at the computer or accessible to it over its LAN;

ii. the toolset makes a determination of and reports the user's system privileges, which can be then used to access data on any associated network or LAN, local files stored on the infected

machine are then also accessed and potentially transmitted over the Internet to a remote site. This may include an upload of the local security database, from which the malware controllers can derive the credentials of any privileged user that ever logged into the infected host computer system. Also the malicious software allows its creators to simply capture and reuse directly from random access memory of the infected host computer, or from a network data stream, the security token or hash of the user, where the user is privileged, and use that token or hash to gain privileged access to other resources on the LAN.

iii. the toolset creates a door that provides remote control and access to the infected system, which allows a remote system unknown to the user of the infected system to control all operations of the host system and have it perform whatever tasks are desired, which may vary between simply downloading data on the infected system to access other websites for denial of service Internet attacks, or a variety of other alternative uses that an enslaved, infected computer can do. This control also allows the remote malicious entity to make a variety of uses of the infected host system. It may even convert the infected host into a source of malicious software itself, causing it to act as another mothership server from which toolsets or secondary payloads are downloaded to other subsequently infected computer systems.

The security and privacy of the user and all confidential information on the user's computer and any associated LAN resources are available to access at this point by the remote entity that controls the operation of the toolset. Even apart from the breach of security, however, the malware, at a minimum, results in a reduction in efficiency of the system due to additional processor demand incurred by the executing malware.

Security systems of various designs have been developed to try to address the problem. For instance, it is possible to use two separate computers, one accessing the Internet and the other connected only with a LAN that is completely isolated from the Internet. This results in a double cost of equipment,

and also there is a problem transferring legitimate data between the machines when necessary and appropriate. Other more software-intensive methods of restricting have also been tried, but these usually expand the demand for bandwidth undesirably, or else do not provide airtight protection against loading of malware.

Summary of the Invention

It is accordingly an object of the present invention to provide a system for a computer that will allow safe browsing without a risk of such infection.

It is further an object of the invention to eliminate the ability of trusted internal host systems on a secure LAN to access the Internet, but to provide access to the Internet through a secure isolated service that can access the Internet, but not the internal trusted LAN sites.

It is further an object of the invention to provide a method for secure file exchange to transfer data between the Internet and the trusted hosts of the trusted LAN.

It is still further an object of the invention to allow Internet access from only the bare minimum of servers or devices in the LAN that require it, and to restrict where they can go.

It is further an object of the invention to provide a system that rigorously monitors any exceptions, including DNS and SMTP exceptions, which might indicate a compromise of any trusted host system on the LAN.

It is also an object of the invention to provide a scalable system that can be applied to a variety of host system architectures or hardware configurations, supporting both laptop and desktop host systems.

According to an aspect of the invention, this is accomplished by a system in which a host computer supports a virtual guest system running thereon. The host system has a firewall thereon such that the host computer cannot communicate directly with the internet, except with predetermined trusted

sites stored in an internal whitelist data. 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 guest 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 interaction is permitted.

According to another aspect of the invention, a networked computer system comprises a local network configured to carry electronic communication signals between computers connected therewith. A connection on the local area network communicates with the Internet, and a plurality of computer stations are each connected with the local network so as to communicate thereacross. Each computer station operates as a host system according to stored data corresponding to an operating system and one or more program applications. The host system communicates over the local network but is restricted against communication with the Internet, except with predetermined Internet sites that have been identified as safe to access. Each computer station also supports operation of a respective virtual computer system thereon. The virtual computer system communicates via a virtual conduit connection over the local area network with the connection to the Internet, but wherein the virtual computer system is isolated against any other communication over the local area network. Each computer station is isolated against any communication of data to or from the respective virtual computer system operating thereon, except for a limited set of types of permitted data transfers.

According to another aspect of the invention, a method of safely browsing the Internet comprises providing a host computer system operating according to a stored operating system and one or more stored program applications, and having operating thereon a firewalled virtual computer system with

which the host computer system has restricted communication of data. The method further comprises accessing the Internet using a first browser program running on the virtual computer system.

According to another aspect of the invention, a computerized work station comprises a computer operatively connected with one or more user-accessible data entry devices, a display device viewable by the user, and computer-accessible data storage providing for the computer an operating system and one or more applications programs that run on said operating system, and supporting a virtual computer system operating on the computer. The computer is able to access the Internet using a browser program running on the virtual computer system such that the browser displays information obtained from the Internet on the display. Data transfers to and from the virtual computer system are limited to a set of types of transfers that limit the possibility of malicious data from the Internet moving from the virtual computer system to another portion of the computer system.

According to still another aspect of the invention, a computer system for browsing the Internet while connected with a local area network comprises a computer having a computer-accessible data storage, an input device connected therewith and a display viewable by a user of the computer. The computer has stored thereon software causing the computer to operate as a host computer system executing application programs and accessing other computerized devices on the local area network, and as a virtual guest computer system operating independently of the host computer system. The host and guest computer systems are able to communicate therebetween only according to a predetermined set of limited interaction processes. The host system has access to the Internet wholly or partially blocked, such that the host system can only communicate with sites that are identified in stored whitelist data. The virtual guest computer system has access blocked to the host computer system and to the local area network. The virtual guest computer system accesses the Internet through the local area network via a virtual conduit to an Internet connection point linked to the local area network.

The above architecture is preferably implemented by commercial-off-the-shelf (COTS) hardware, all of which is readily available. The computers described herein and the networks, both local area and the internet, rely on the standard well known network hardware now in common use. The separate internet access for the virtual guest is preferably provided by a COTS system used in virtual private networks (VPNs). The firewalls and other communication restrictions of the system are implemented preferably by software, i.e., using computer-readable instructions stored on the computer systems that cause those computer systems to operate according to the firewall and communications architecture as described herein.

According to an aspect of the invention, this is accomplished by providing a host computer that is surrounded by a host based firewall. The firewall allows the host to access addresses on the LAN but blocks any access to any address on the Internet, except for Internet addresses that are specifically whitelisted, i.e., predetermined to be trusted sites. In the preferred embodiment, the firewall *inter alia* prevents or disables any access to the usual Internet access ports, e.g., ports 80 and 443, which are also the ports that are usually used by executing stub code of an infection to access the Internet without knowledge of the user. Because these are also the usual ports used to access the Internet by a browser in ordinary use in the prior art, the host computer consequently does not have any direct contact to and cannot communicate with the Internet through its ports, except that the host computer is permitted to access other sites on the secure LAN itself through these ports, and also trusted Internet sites that are predetermined and stored in whitelist data accessible to the host computer (or to the LAN firewall).

Also operating on the host computer is a hypervisor system that creates a virtual machine environment that is separate from the host computer's operating system. This virtual machine has a virtual guest operating system on which a modified browser is run. The browser is activated by a desk-top shortcut or application on the host system that allows the user to link to the isolated Internet access of the virtual guest system by launching the virtual guest web browser, which operates transparently to the user in the virtual guest system.

The virtual guest system browser is configured to access the Internet *only* through a specific and unique Internet access point identified by a unique IP address, e.g., 10.1.xxx.xxx, or 255.255.2xx.xxx, for that specific virtual guest system. The virtual guest system has, as part of its virtual architecture, ports 80 and 443, and generally operates internally as a normal browser, except that it relies on a dedicated connection to get to the Internet. Because it is exposed to potentially malicious software as it browses the Internet, the virtual guest system browser and its virtual operating system may be a hardened version that is exceptionally resistant to corruption, or it may have enhanced anomaly detection to aid in noting when dangerous data has been encountered by the browser. The virtual guest system also has no connection whatsoever to the LAN, and cannot access any address on the LAN.

In the preferred embodiment, the unique IP address is provided by a virtual private network (VPN) termination point device on the LAN that is connected to the virtual guest system and its browser through the LAN by a VPN. In this LAN embodiment, the host computer firewall allows the host computer to communicate only with IP addresses on the LAN, and the host computer can only communicate with the Internet through the virtual guest system communicating through the VPN to the VPN termination point. The VPN termination point is connected by a local hardwired connection to the firewall between the LAN and the Internet, and it connects directly to the firewall without passing through the LAN. Consequently all Internet traffic from the host computer is restricted to run only from the virtual guest system through the sealed conduit of the VPN, and then through the firewall and into the Internet at large. There is no contact between the Internet traffic and the LAN.

The virtual guest system browser may alternatively be connected to the Internet access point directly as a local hardware device connected directly to the host computer without an intervening network or LAN. In this embodiment, a single computer connected directly to an Internet access point may be provided with protection against malware in the absence of a trusted local network.

The guest computer and the host computer communicate with each other by a limited permissible internal host-based firewall in the host system that is provided by the hypervisor or some other local program. Communications across this internal firewall between the guest system and the host system are limited to cut and paste of displayed documents or files, commands to print documents, and file transfer requested manually by the host (i.e., directed intentionally by the human user of the given system).

As a result of this arrangement, should the guest browser system access a website that returns some malware stub code over the Internet, the stub code is executed on the guest browser. The guest browser will then access the "mother ship" site with the secondary malware payload via its virtual ports 80 or 443 as directed to by the stub code software, and it will download the secondary payload executable module onto the virtual guest machine, which is configured by the hypervisor as essentially a blank PC with a browser and isolated from the real host computer. The secondary payload will then run on and access the virtual or pseudo guest machine, which has no files or system assets that are usable for the infection of a system.

The guest system is compromised at this point. However, the guest computer in the virtual machine has no access to the other computers on the network or even to the system assets or files of the host system itself, except to cut, paste, or print. This is the limit of the infection, and there is no compromise to the host system security.

The compromised guest system may start to encounter problems, and might even become inoperable with the malware running if it is forced to function as a netbot or remote controlled device working for the mother ship site. However, the hypervisor stores a pristine copy or clean slate of the entire virtual guest system, and that pristine copy can be reloaded in place of the existing virtual guest machine, either periodically, e.g., once a day or once an hour, or on command of the user when there might be an infection. The infected virtual guest system therefore can be cleared immediately and reverted to its original condition without any harm to the actual host computer.

Even if malware were to get through the firewall and initiate an executable module on the host operating system instead of the virtual guest system, such as by a virus attached to an email or contamination by a USB memory stick or other hardware device that introduces a virus to the host operating system behind the host firewalls, nonetheless the malware module would not be able to access the Internet because the ports on the host machine are disabled for Internet access. With the malware unable to communicate outside the local area network, there would be no exfiltration of data, and malware beaconing, or any possibility of remote command and control. Furthermore, the blocked attempts to access the generally disabled or blocked ports 80 or 443 (or whatever other ports may appropriately be disabled or blocked) can be detected as an indication that the host computer is infected. If an infection is detected, then the host system could then be scrubbed or rebuilt, and the security compromise would have had only minimal effect.

Other advantages of this invention will become apparent from the foregoing specification.

Brief Description of the Drawings

Figure 1 is a diagram of an exemplary system on a local area network using the Internet isolation system of the present invention.

Figure 2 is a diagram of a stand-alone computer system that is protected from infection from Internet sites by an architecture according to the present invention.

Detailed Disclosure of the Invention

Referring to Figure 1, a networked computer system generally indicated at 1 is linked to the Internet 5 via a firewall 3 and a router 2 of conventional configuration that is well-known in the art. A proxy/ web-content filter 4 is connected with and cooperates with the firewall hardware 3 to control the type of data permitted to pass from the Internet 5 into the local system 1, filtering e.g., pornographic material or data not intended for the system 1, and also blocks communications from users on the LAN

trying to reach disallowed sites, e.g., requests to access www.onlinecasino.com.The local system 1 includes a trusted local area network (LAN) 7 that transmits electrical data signals between a plurality or large number (not shown) of computer systems each identified by a unique LAN address. The computers include at least one workstation or laptop generally indicated at 9. Each of the computers on the LAN 7 is configured similarly to the computer system 9 to prevent malware intrusion from the Internet.

The workstation 9 can be virtually any host computer system, including a PC or a laptop or any of a variety of other computer systems with electronically accessible data storage, a user visible display, and input devices such as a keyboard and a mouse. As an example, the system may be a PC sold by Dell, with 4GB RAM and 146 GB hard disk storage, a monitor, a keyboard and a mouse. The host system 9 stores thereon data providing an operating system that allows the host system 9 to function, e.g., a Windows or Linux operating system, as is well known in the art. It also stores data corresponding to all of the software needed for operation of the computerized workstation 9 in common operation, e.g., word processing programs, accounting programs, or any application that is supported on a computer. Also, the host computer system has a browser program that may be modified to enhance operation with a guest system, as will be discussed below.

The host system 9 also has stored data in the form of software instructions that cause the host system to have a host-based firewall 11 that provides restrictive egress from the computer 9. This host-based firewall 11 may be implemented using software such as, for example, that sold under the names Symantec Endpoint Protection or MacAfee Host-Based Security Systems.

This host based firewall 11 blocks all communications from the computer 9 except that it permits passage through it only of communications to the IP addresses of other computers on the trusted network 7. The firewall 11 specifically does not permit the computer 9 to access ports 80 or 443, and potentially also prevents access to ports 27 and to 77, and to any other ports that may or may become vulnerable to malware or security threats at some point in the future. This firewall 11 may allow the computer 9 only

some limited use of these ports if the communication is purely with pre-determined trusted Internet sites, as will be described below. This firewall 11 is therefore a preventive barrier to any access of the Internet from host system 9 through its ports or directly to the firewall 3 via the LAN.

Host system 9 stores data defining software that when executed creates a hypervisor on the computer system 9. The hypervisor may be one of a variety of types of hypervisor, either software that executes directly as a separate operating system on the hardware of computer 9, or as a software module that operates based on the underlying operating system, e.g.,. Windows 7, of the computer 9. In either case, the hypervisor effectively creates a virtual machine operating on the host computer that has a virtual configuration different from the real hardware and software configuration of the computer 9. The hypervisor employed may include software packages or modules such as Med-V from Microsoft, Invincea, Microsoft – Virtual PC 2007 or Hyper-V, VMWare Player or ESX, or SUN Microsystems XVM Virtual Box. The virtual machine created by the hypervisor is illustrated in the diagram of FIG. 1 as the virtual guest system or guest OS 13.

In addition to forming the virtual guest system 13, the hypervisor also provides an additional internal host-supported firewall indicated at 15 that separates and restricts interaction between virtual guest system 13 and the trusted-host operating system 17, which is the standard operating system running the host computer 9, e.g., Windows 7 or another system that will support or cooperate with the hypervisor. Communications between the trusted host OS 17 and the guest OS 13 pass through the hypervisor firewall 15, and are limited to:

1. Cutting or copying of text visible on the screen;

2. Pasting of the text that has been cut or copied from what is visible on the screen;

3. Receiving a queued request lodged with the hypervisor by the guest OS 13 that the host system print files on a printer (not shown) connected with the workstation or laptop 9 , and;

4. Transfer of files, when directed by the host computer OS 17, between a computer memory area (such as a respective desktop) or virtual data storage accessible to the virtual guest OS 13 and a computer memory area (such as a respective desktop) or data storage accessible to the host OS 17.

The guest OS pseudo machine or virtual guest system 13 is has its own virtual architecture and configuration. It preferably has virtual architecture of a very simple or gutted PC with a desktop area that can be accessed manually by a user of the computer system 9 to transfer files to be accessed by the virtual guest browser, but few if any associated system assets or I/O devices. The only files in the virtual machine 13 are those in its own desktop. The virtual guest system 13 shows no software installed except for a browser and possibly some related supportive software, such as Adobe or Windows Media Player that cooperate with the browser when certain types of files are accessed on the Internet, and potentially an email program such as Microsoft Outlook for certain configurations.

File transfer to and from the virtual guest system is very restricted, and can only occur in response to a user input directing the transfer. This allows for download and upload of documents, but the process requires slightly more user action than in an unprotected system of the prior art.

If a user is browsing and wishes to download a file from the Internet, the user will left click for download, as is standard in the art, and a dialog box will open in the browser in the guest system, asking the user where to store the file and under what name. The area available to store is a virtual data storage space that can be organized with folders by the user, as is well-known in the art. The user selects a file name and downloads the file into that virtual area. The user then goes to the Start Menu on his host computer, and this will offer him as one of the application choices "File Transfer". When selected and clicked, this will open a window similar to Windows Explorer displaying the files of the virtual data storage area of the virtual guest system. The user can select the file and copy it to any data storage area of the host system. The file then becomes available to the host and for access over the trusted LAN.

If a user wishes to upload a file to an Internet site, the user again accesses the File Transfer application running on the host system, and then copies the file form the data location in the host system into the virtual data storage of the virtual guest system. The browser than can be opened and when the browser dialog box opens in the guest system, the virtual data storage area of the guest is visible, and the file is visible there to be selected for uploading by the browser.

The host OS 17 has a desktop displayed to the user that includes an icon corresponding to the browser that runs in the virtual guest system 13. When this icon is clicked on by the user, it initiates the browser program running in the virtual guest system 13. The browser may be Firefox or Internet Explorer 6, 8 or whatever version of these is available, and other browsers may also be used with similar advantage. The virtual guest system 13 includes in its virtual architecture ports 80 and 443, access to which is permitted in the virtual guest system 13. These ports function to access the Internet, but the traffic does not go through real hardware ports on the host computer 9. Rather, the traffic between the Internet and the browser of the virtual guest system 13 is routed through a sealed "virtual conduit" 19 passing through the LAN. The virtual guest system 13 is able to communicate using its browser through only one mechanism, i.e. the virtual private network connection indicated at 19 that allows for the guest operating system to communicate over the trusted network 7 to a VPN termination point that is located adjacent the enterprise firewall 3.

This virtual conduit is really a software-generated Virtual Private Network (VPN) tunnel that encrypts data passing to and from the Internet and ensures that it is received or delivered to the virtual guest system 13 at one end and at VPN termination point 21 at the other end, without the possibility that the data thereof can reach any other location in the LAN except those two locations. The virtual guest system 13 uses Network Address Translation to support a captive VPN session to the VPN termination point 21. The VPN 19 is basically a tamper-proof conduit through the local area network 7 that prevents any contamination passing from the Internet to the guest OS or back outward from reaching any other

system on the local area network. It can be analogized to a pipe full of toxin passing through an otherwise clean water supply.

The VPN termination point may be connected with the firewall 3 or integrated into it. Appropriate VPN termination point hardware devices are off-the-shelf systems such as the Check Point UTM-1 570, the Cisco ASA 5510 or Juniper Networks NetScreen. The VPN transmits data packets that are encrypted according to an IPSEC or SSL VPN tunnel construct protocol. The data in the VPN is transmitted over the LAN from the virtual guest system 13 on the host computer 9 in this encrypted form to the VPN termination point 21, where it is decrypted for transmission to the Internet. The VPN termination point includes hardware that is physically connected with the firewall device 3 outside of the LAN, not connecting with the firewall 3 through the LAN, and the VPN termination point includes in the data transmitted data defining a unique IP address for the specific virtual guest system 13, e.g., 10.1.xxx.xxx, or 255.255. 2xx.xxx. This gives the appearance to the receiving Internet server that the virtual guest system 13 is not an IP address on a LAN, but a solitary PC without a LAN.

Similarly, data packets received from the Internet directed to the virtual guest system 13 pass through the firewall 3 and other standard prior art security measures applied where the Internet meets the LAN, such as filter 4, and these packets are then encrypted at the VPN termination point and then sent encrypted through the LAN to the host computer 9. At the host computer 9 at the other end of the VPN they are received and passed to the virtual guest system 13, where the data is decrypted and displayed by the browser.

The guest OS 13 can be easily infected or compromised and made unusable by the malware or other threats that it is exposed to. The browser is consequently preferably hardened to reduce its volatility in the face of such attacks. In addition, the hypervisor retains a virtual image of the virtual guest system 13 in its original pristine state free of any infections or history, so that the virtual guest system 13 can easily be reset to its pristine clean state, i.e., a clean slate, by reloading the data defining the uninfected

virtual guest system 13. This is preferably done frequently in the system, e.g. once a day, so that there are no persistent infections that may develop in the virtual guest system 13.

It may occur that software installed on the host machine 17 requires live access to the Internet for proper operation of the software. For example, some software requires access to a certificate online to be executable. Similarly, access to online help from a software module requires that the host computer access the relevant websites. In either case, the host OS 17, not the guest OS 13 must access the Internet. To allow for this, the firewall 11 around the host OS 17 selectively enables the host OS 17 to access the Internet directly through ports 80 or 443, which are otherwise disabled, provided that the websites being accessed are on a whitelist of predetermined trusted sites with which the host OS 17 is permitted to communicate with.

The email program for the workstation 9 may be operated as a sort of browser application in the virtual guest system, with emails retained in the virtual guest system. Alternatively, where the LAN includes a server inside the LAN for email, the email program may be run on the host OS.

The host computer system can in some cases be disconnected from the LAN and connected with a different network, as when a laptop is taken by a user to a remote location, such as, for example, to a hotel where it accesses the Internet using a different network. The host based firewall 11 (HBFW) remains on the computer system 9, but performs multiple predetermined functions based on whether the computer 9 is "home" (attached to the LAN) or "roaming" (disconnected from the LAN and connected via a non-secure network to the Internet).

At home on the LAN:

The guest system, when the host is "home" on the trusted LAN network, is allowed by the HBFW only to egress the network through the VPN endpoint via a specified IP address using a predetermined port/protocol (i.e. UDP 500 or TCP 10000)

The home system, when the host is "home" on the trusted LAN network, is allowed by the HBFW to communicate to other LAN resources as well as any whitelisted sites outside the LAN on the Internet. All other egress ports/protocols/paths are blocked. If not, a malicious program could try and connect to a "mothership" via port 21, which is a well known port often allowed for access the internet for file transfers. It is possible for the IT personnel to configure the system to specifically allow or whitelist other ports or websites for necessary or reasonably permitted file transfers to known entities.

When roaming:

The guest, when off the trusted network, is allowed by the HBFW to freely communicate on whatever network it is connected to. As a result, if the system is a laptop connecting to the Internet in a hotel room or via a Wi-Fi network, the computer system 9 can still connect to the Internet without requiring the VPN.

The host, when roaming on a nonsecure network, has all egress blocked by the HBFW.

LAN Firewall:

In addition to the HBFW, the LAN has LAN firewall 3, which further secures the local area network. On the network, it is not possible to determine if it is the guest or the host trying to communicate, because since both the host and the guest use the host IP address. (The guest uses the NAT'd TCP/IP network address assigned to the host).

This LAN firewall device 3 is configured to block all host-based egress for all ports, protocols and destinations, with the exception of the following:

i. the guest system can access the VPN endpoint using the host's NAT'd TCP/IP network address and will use a predetermined port/protocol (i.e. UDP 500 or TCP 10000)

ii. Host egress is permitted via specified ports/protocols (80, 443) to any predetermined whitelisted sites that are required by host.

The LAN firewall does not address LAN access because the firewall is usually installed at the edge of the LAN to filter egress/ingress from the LAN, and is not between the host and any other IP address on the LAN.

FIG. 2 shows an alternate embodiment of the invention with a single system attached to the internet without a LAN. FIG. 2 shows a number of components similar to those in FIG. 1, and in FIG. 2 similar parts have the same reference character numbers as in FIG. 1.

In the embodiment of FIG. 2, a computer system 23, such as a standard PC sold by Dell as described above, is connected with the Internet 5 through a router 2 and a firewall 3 as described above. Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, as above.

Computer system 23 has an internal architecture similar to the system 9 of the first embodiment. The system 23 includes a host system 25 running on the resident operation system, such as Windows or Linux, and a virtual guest system 27 defined by a hypervisor program running on the computer 23. The host and guest systems 25 and 27 are separated by an internal firewall 29 defined by the hypervisor that restricts the interaction between the host and guest in the same way that the firewall 15 of the first embodiment restricts communication between its host and guest systems.

The computer system 23 is also provided with a firewall 31 that limits communications from the host system 25. The host system 25 is blocked from communicating with any IP address, *except* that host system can communicate through the firewall 31 via a local hardwired connection to firewall 3 and through router 2 to access any sites on the Internet 5 that have been predetermined to be whitelisted or trusted sites, such as software certificate sites or software online help sites, as discussed above.

Because there is no LAN, the system 23 does not make use of a VPN. Virtual guest system 25 communicates over a hardwired connection to a VPN termination point device that gives the guest an IP address when browsing on the Internet. The firewall 31 allows the guest system 27 to communicate without restriction with any site on the Internet 5.

The hypervisor of the system 23 has a refresh or clean slate restoration process that restores the virtual guest system 27 to its original pristine state periodically, e.g., every 24 hours, or when an infection is detected or suspected, or simply responsive to a manual directive input from the user at the user's discretion.

This embodiment also provides protection against Internet malicious software threats by its isolation of the host system.

In a particularly preferred embodiment, the host and guest systems each have browser programs installed that facilitate access to the Internet without risk to the separation of the host from the virtual machine.

The host 17 runs a browser, which may be any typical browser, such as e.g., Internet Explorer, Mozilla Firefox, etc. The host browser has access to stored data defining a whitelist of trusted destination resources, usually IP addresses or sites, including the other accessible sites on the secure LAN and trusted sites on the Internet. An add-on checks for each address or site accessed whether it is on the whitelist. If so, the host browser accesses that address or site, and that is permitted by the host firewall 11 and the LAN firewall 3 if it is on the Internet. If the address that the host browser is trying to access is not a trusted LAN or Internet site in the whitelist data, the host browser immediately transfers the address or site to which access is sought to the guest browser.

The guest browser may be already running or it may be started by the host browser add-on. The guest browser will open to display the site to the user to be viewed in the guest browser, and then go to the non-whitelist site as discussed above, via the VPN or the non-firewalled connection to the Internet.

Ex.1002
CISCO SYSTEMS, INC. / Page 20 of 517

Any malware or other deleterious data or code on the non-trusted site will be processed as above, remaining isolated in the guest computer system, unable to cross over the firewall back into the host computer.

The host monitors the guest browser at all times and screens any destination resource or address that the guest browser tries to access. If the there is an attempt to access a trusted whitelist site in the guest browser, then the host browser takes over the request clears the request in the guest browser. The host browser then opens on the user's display, and the request to access the trusted site will be processed from the host browser. Careful screening of the DNS, SMTP or other aspects of the communication is monitored by the firewalls to ensure that the system is not misled into communicating with an unsafe site directly from the host computer 17.

All the other aspects of the firewall 15 described previously are fully maintained to keep the systems isolated. Specifically, data from sites that are opened by the virtual guest system browser remains isolated in the virtual system behind the internal firewall 15, and can only be moved by the limited types of transfer described above, i.e., cut, copy, paste, print, etc.

While the present system relies on software implementations of many of the aspects of the invention, it will be understood that hardware analogues of the software implementations may also be employed.

The terms used herein should be seen to be terms of description rather than of limitation, as those of skill in the art with this disclosure before them will be able to make modifications and revisions thereto without departing from the spirit of the invention.

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

Listing of Claims:

1-27. (Cancelled)

28. (New) A networked computer system comprising:

a network;

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.

29. (New) The networked computer system of claim 28, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input.

30. (New) The networked computer system of claim 28, wherein the host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space.

31. (New) The networked computer system of claim 28, wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system.

32. (New) The networked computer system of claim 28, wherein the computer system is configured to:

communicate with the one or more untrusted network destinations via a first communication connection,

communicate with one or more trusted network destinations via a second communication connection; and

enforce separation of the first communication connection from the second communication connection.

33. (New) 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.

34. (New) 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.

35. (New) 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.

36. (New) 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.

37. (New) 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.

38. (New) A method of network isolation in a networked computer system, the method comprising:

providing a network and at least one computer system that is 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;

separating the host system from the virtual system using an internal firewall executed on the computer system;

implementing network isolation between the computer system and the network using a host-based firewall executed on the computer system;

providing at least one device configured to implement a network firewall or a web proxy; and

implementing network isolation, between one or more untrusted network destinations and the networked computer system, via the at least one device.

39. (New) The method of claim 38, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input.

40. (New) The method of claim 38, further comprising:

the host system storing data in a host data storage; and

the virtual system storing data in a virtual data storage.

41. (New) The method of claim 38, further comprising preventing malware introduced to the computer system from moving to another computer system of the networked computer system.

42. (New) The method of claim 38, further comprising:

communicating with the one or more untrusted network destinations via a first communication connection;

communicating with one or more trusted network destinations via a second communication connection; and

enforcing separation of the first communication connection from the second communication connection.

43. (New) The method of claim 38, further comprising preventing, via the host-based firewall, lateral communication and movement of malware between the computer system and other devices on the networked computer system.

44. (New) The method of claim 38, further comprising the at least one device preventing unauthorized communication between the computer system and the one or more untrusted network destinations.

45. (New) The method of claim 38, further comprising:

implementing a first policy for the host-based firewall when the computer system is connected to the network, the first policy for the host-based firewall permitting one or more communications between the host system of the computer system and one or more resources on the network; and

implementing a second policy for the host-based firewall when the computer system is connected to another network, the second policy for the host-based firewall blocking communications egressing from the host system of the computer system but allowing communications egressing from the virtual system.

46. (New) The method of claim 38, further comprising running one or more applications or processes in the virtual system that are configured to communicate with the one or more untrusted network destinations.

47. (New) The method of claim 38, further comprising running one or more applications or processes in the host system that are configured to communicate with one or more devices on the network.

Ex.1002
CISCO SYSTEMS, INC. / Page 26 of 517

WHAT IS CLAIMED IS:

1. A networked computer system comprising:

a local network configured to carry electronic communication signals between computers connected therewith; and

a connection on the local area network communicating with the Internet; and

a plurality of computer stations each connected with the local network so as to communicate thereacross;

each computer station operating as a host system according to stored data corresponding to an operating system and one or more program applications, said host system communicating over the local network but being restricted against communication with any destination resource, except with predetermined destination resources that have been identified as safe to access;

each computer station also supporting operation of a respective virtual computer system thereon, said virtual computer system communicating via a virtual conduit connection over the local area network with the connection to the Internet, but wherein the virtual computer system is isolated against any other communication over the local area network;

each computer station being isolated against any communication of data to or from the respective virtual computer system operating thereon, except for a limited set of types of permitted data transfers.

2. The networked computer system of claim 1, wherein the connection communicating with the Internet includes for each computer station a respective virtual private network termination

device that gives the virtual computer system an IP address on the Internet that indicates it to be a single computer system having fewer resources than the corresponding computer station.

3. The networked computer system of claim 2, wherein a firewall is interposed between the Internet and the virtual private network termination device and the local area network, and said firewall blocks communications with the Internet via the LAN, but does not interfere with communications between the virtual private network termination device and the Internet.

4. The networked computer system of claim 1, wherein the computer station is a computer work station or a laptop computer.

5. The networked computer system of claim 1, wherein the host system is blocked against communicating with any site over the Internet except for sites defined by predetermined whitelist data identifying trusted sites on the Internet.

6. The networked computer system of claim 1, wherein the host system is at least partially blocked against communicating via specified ports of said computer station by a firewall between the host system and the local network, or a firewall between the local network and the Internet.

7. The networked computer system of claim 1, wherein the host system is blocked against communicating via ports 80 or 443 with any destination resource except for destination resources defined by predetermined whitelist data identifying trusted destination resources on the Internet.

8. The networked computer system of claim 1, wherein the virtual computer system is defined by a hypervisor program running on the computer station that isolates the virtual computer system from the host computer system.

9. The networked computer system of claim 1, wherein the user of the computer station activates the virtual computer system by starting an internet browser program that runs in the virtual computer system.

10. The networked computer system of claim 1, wherein the computer station stores data defining a pristine version of the virtual computer system, and the user of the computer station can interface therewith and instruct the computer station to restore the virtual computer system to the pristine version.

11. The networked computer system of claim 1, wherein the set of permitted data transactions is a set of one or more elements selected from the group consisting of

a. cutting or copying text displayed on the display;

b. pasting text that has been cut or copied from the display;

c. receiving a request to print a file on a local printer; and

d. transferring files between a data area associated with the host and a data area associated with the virtual computer system.

12. A method of safely browsing the internet, said method comprising:

providing a host computer system operating according to a stored operating system and one or more stored program applications, and having operating thereon a firewalled virtual computer system with which the host computer system has restricted communication of data; and

accessing the Internet using a first browser program running on the virtual computer system.

13. The method of claim 12, wherein said host computer system is firewalled against access via predetermined ports of the host computer system to any sites on the Internet, except for

predetermined trusted sites identified in whitelist data stored so as to be accessible to the host computer system, said method further comprising

14. determining possible infection of the host computer system responsive to a detection of the host computer system accessing one or more of said predetermined ports. The method of claim 12, wherein the virtual computer system is created by a hypervisor program stored as data accessible to and running on the host computer system, said method further comprising:

storing an original version of data defining the virtual computer system and software running thereon; and

restoring the virtual computer system to said original version thereof responsive to input instruction from a human user or periodically.

15. The method of claim 12, wherein the communication of data between the host and virtual computer systems is restricted so as to be limited to transfers of data selected from the group consisting of

a. cutting or copying text displayed on a display connected with the host computer system;

b. pasting text that has been cut or copied from the display;

c. receiving a request to print a file on a local printer connected with the host computer system; and

d. transferring files between a data area associated with the host computer system and a data area associated with the virtual computer system.

16. The method of claim 12, wherein said accessing of the Internet is via a virtual conduit through a local area network between the virtual computer system and a VPN termination point linked to the Internet.

17. The method of claim 12, wherein the host computer system is connected with a display device viewable by a human user thereof, said method further comprising displaying images derived from the Internet by the first browser program on said display device.

18. The method of claim 17, wherein a second browser program runs on the host computer system and receives input from the user thereof directing the second browser program to access sites in the local network or on the Internet, said method further comprising:

determining, responsive to a directive of the user to access a specified site, whether or not the site is one of a predetermined set of whitelisted sites defined by data accessible to the second browser program; and

responsive to said determination, accessing the specified site with the first browser program running on the virtual computer system if the site is not one of said set of whitelisted sites, or accessing the specified site with the second browser program running on the host computer system if the site is one of said set of whitelisted sites; and

displaying the data obtained to the user using the browser program used.

19. A computerized work station comprising:

a computer operatively connected with one or more user-accessible data entry devices, a display device viewable by the user, and computer-accessible data storage providing for the computer an operating system and one or more applications programs that run on said operating system, and supporting a virtual computer system operating on the computer;

said computer being able to access the Internet using a browser program running on the virtual computer system such that the browser displays information obtained from the Internet on the display; and

wherein data transfers to and from the virtual computer system are limited to a set of types of transfers that limit the possibility of malicious data from the Internet moving from the virtual computer system to another portion of the computer system.

20. The computerized work station according to claim 19, wherein the workstation is a laptop computer.

21. The computerized work station according to claim 19, wherein, apart from access via the browser of the virtual computer system, access of the computer to any sites on the Internet except for sites identified by a predetermined set of trusted sites is blocked by a firewall.

22. The computerized work station according to claim 19, wherein any communications via ports 80 and 443 of the computer are blocked, except for communications with sites that are identified by a predetermined set of trusted sites in stored whitelist data.

23. The computerized work station according to claim 19, wherein the virtual computer system is operated as a virtual machine of a hypervisor machine.

24. The computerized work station according to claim 19, wherein the computer accesses the internet via a virtual conduit through a local area network leading to a VPN termination point linked to the Internet.

25. The computerized work station according to claim 19, wherein the data transfers are limited to cut instructions, copy instructions, paste instructions, print requests and file transfer instructions initiated by a user accessing the computer manually.

Ex.1002
CISCO SYSTEMS, INC. / Page 32 of 517

26. A computer system for browsing the Internet while connected with a local area network, said computer system comprising:

a computer having a computer-accessible data storage, an input device connected therewith and a display viewable by a user of the computer;

said computer having stored thereon software causing the computer to operate as a host computer system executing application programs and accessing other computerized devices on the local area network, and as a virtual guest computer system operating independently of the host computer system, said host and guest computer systems being able to communicate therebetween only according to a predetermined set of limited interaction processes;

said host system having access to the Internet wholly or partially blocked, such that the host system can only communicate with sites that are identified in stored whitelist data;

said virtual guest computer system having access blocked to the host computer system and to the local area network, and

said virtual guest computer system accessing the Internet through the local area network via a virtual conduit to an Internet connection point linked to the local area network.

27. The computer system of claim 26, wherein access of the host system to the Internet is blocked by a firewall that prevents access to all Internet sites except predetermined trusted sites, and that disables communications over ports 80 and 443, and data transfer between the host and guest computer systems is limited to cutting text, copying text, pasting text, transmitting files to be printed at a printed locally attached to the computer system, and manual transfer of files into and out of a virtual storage area of the guest computer system.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2012 (02.08.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/103517 A1

(51) International Patent Classification:
G06F 21/22 (2006.01)

(21) International Application Number:
PCT/US2012/023027

(22) International Filing Date:
27 January 2012 (27.01.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/436,932 27 January 2011 (27.01.2011) US

(71) Applicant *(for all designated States except US)*: **L-3 COMMUNICATIONS CORPORATION** [US/US]; 600 Third Avenue, New York, NY 10016 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **HOY, Robert, B.** [US/US]; 241 Barnsboro Road, Sewell, NJ 08080 (US). **FENKNER, Mark** [US/US]; 115 Cottonwood Drive, Marlton, NJ 08053 (US). **FARREN, Sean, W.** [US/US]; 62 Boardner Street, Newburyport, MA 01950 (US).

(74) Agent: **TIAJOLOFF, Andrew, L.**; Tiajoloff & Kelly LLP, Chrysler Building, 37th Floor, 405 Lexington Avenue, New York, NY 10174 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU,

[Continued on next page]

(54) Title: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

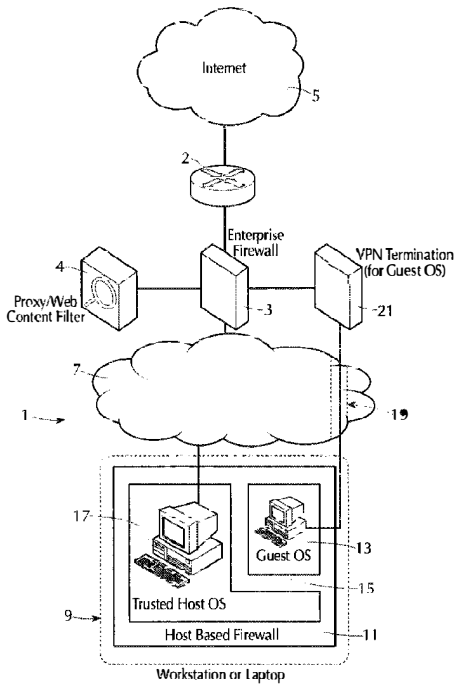


FIG. 1

(57) 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.

WO 2012/103517 A1

TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

DOCKET NO.: LCOM_ISO_US02 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
L3 TECHNOLOGIES, INC.

For: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

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

AUTHORIZATION TO TREAT A REPLY AS INCORPORATING AN EXTENSION OF TIME UNDER C.F.R. § 1.136(a)(3)

Sir/Madame:

The Commissioner is hereby requested to grant an extension of time for the appropriate length of time, should one be necessary, in connection with this filing or any further filing submitted to the U.S. Patent and Trademark Office in the above-identified application during the pendency of this application. The Commissioner is further authorized to charge any fees related to any such extension of time to Deposit Account No. 50-5519.

Date: March 2, 2018

/Joseph R. Klinicki/
Name: Joseph R. Klinicki
Registration No.: 68,505

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **L3 TECHNOLOGIES, INC.**	**Confirmation No.: Not Yet Assigned**
Application No.: Not Yet Assigned	**Group Art Unit: Not Yet Assigned**
Filing Date: Herewith	**Examiner: Not Yet Assigned**

For: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

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

Sir:

PRELIMINARY AMENDMENT PURSUANT TO 37 CFR § 1.115

Preliminary to examination of the above-captioned patent application, please amend the application as follows:

☒ **Amendments to the Specification** begin on page 2 of this paper.

☒ **Amendments to the Claims** are reflected in the listing of the claims which begins on page 3 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 8 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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

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

Secrecy Order 37 CFR 5.2:

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

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Robert	B.	Hoy	

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

City	Sewell	State/Province	NJ	Country of Residence	US

Mailing Address of Inventor:

Address 1	600 Third Avenue		
Address 2			
City	New York	State/Province	NY
Postal Code	10016	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Mark		Fenkner	

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

City	Marlton	State/Province	NJ	Country of Residence	US

Mailing Address of Inventor:

Address 1	600 Third Avenue		
Address 2			
City	New York	State/Province	NY
Postal Code	10016	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sean	W.	Farren	

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

City	Newburyport	State/Province	MA	Country of Residence	US

Mailing Address of Inventor:

Address 1	600 Third Avenue		
Address 2			
City	New York	State/Province	NY
Postal Code	10016	Country	US

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

Correspondence Information:

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

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

Customer Number	15027		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS		
Attorney Docket Number	LCOM_ISO_US02	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	2	Suggested Figure for Publication (if any)	1

Filing By Reference:

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

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

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

Publication Information:

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

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

Representative Information:

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

Please Select One:	(●) Customer Number	( ) US Patent Practitioner	( ) Limited Recognition (37 CFR 11.9)
Customer Number	15027		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	13981896	2013-07-29
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13981896	a 371 of international	PCT/US2012/023027	2012-01-27
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
PCT/US2012/023027	Claims benefit of provisional	61436932	2011-01-27

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

Foreign Priority Information:

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

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

Remove

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

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

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

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

Applicant Information:

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

Applicant 1

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

Clear

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

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

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	L3 TECHNOLOGIES, INC.

Mailing Address Information For Applicant:

Address 1	600 Third Avenue		
Address 2			
City	New York	**State/Province**	NY
Country	US	Postal Code	10016
Phone Number		Fax Number	
Email Address			

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

Assignee Information including Non-Applicant Assignee Information:

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

Assignee 1

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

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

Organization Name	L3 TECHNOLOGIES, INC.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	600 Third Avenue		
Address 2			
City	New York	**State/Province**	NY
Country[i]	US	Postal Code	10016
Phone Number		Fax Number	
Email Address			

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

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Joseph R. Klinicki/			Date (YYYY-MM-DD)	2018-03-02
First Name	Joseph R.	Last Name	Klinicki	Registration Number	68,505

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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ISO_US02
	Application Number	
Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS	

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

Privacy Act Statement

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

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

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

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

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

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

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

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.

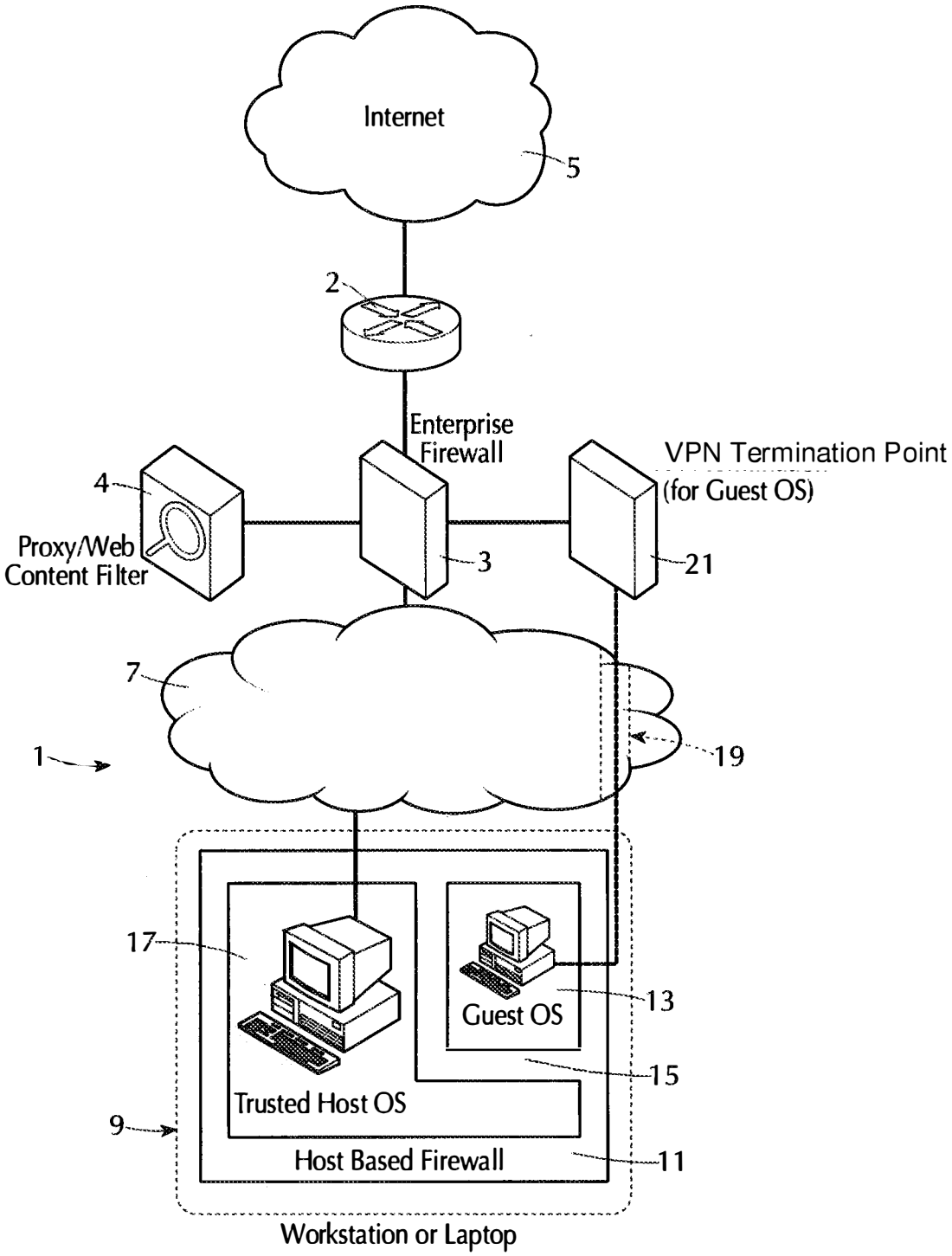

Internet
5
2
Enterprise
Firewall
VPN Termination Point
(for Guest OS)
4
Proxy/Web
Content Filter
3
21
7
1
19
17
Guest OS
13
15
Trusted Host OS
9
Host Based Firewall
11
Workstation or Laptop

FIG. 1

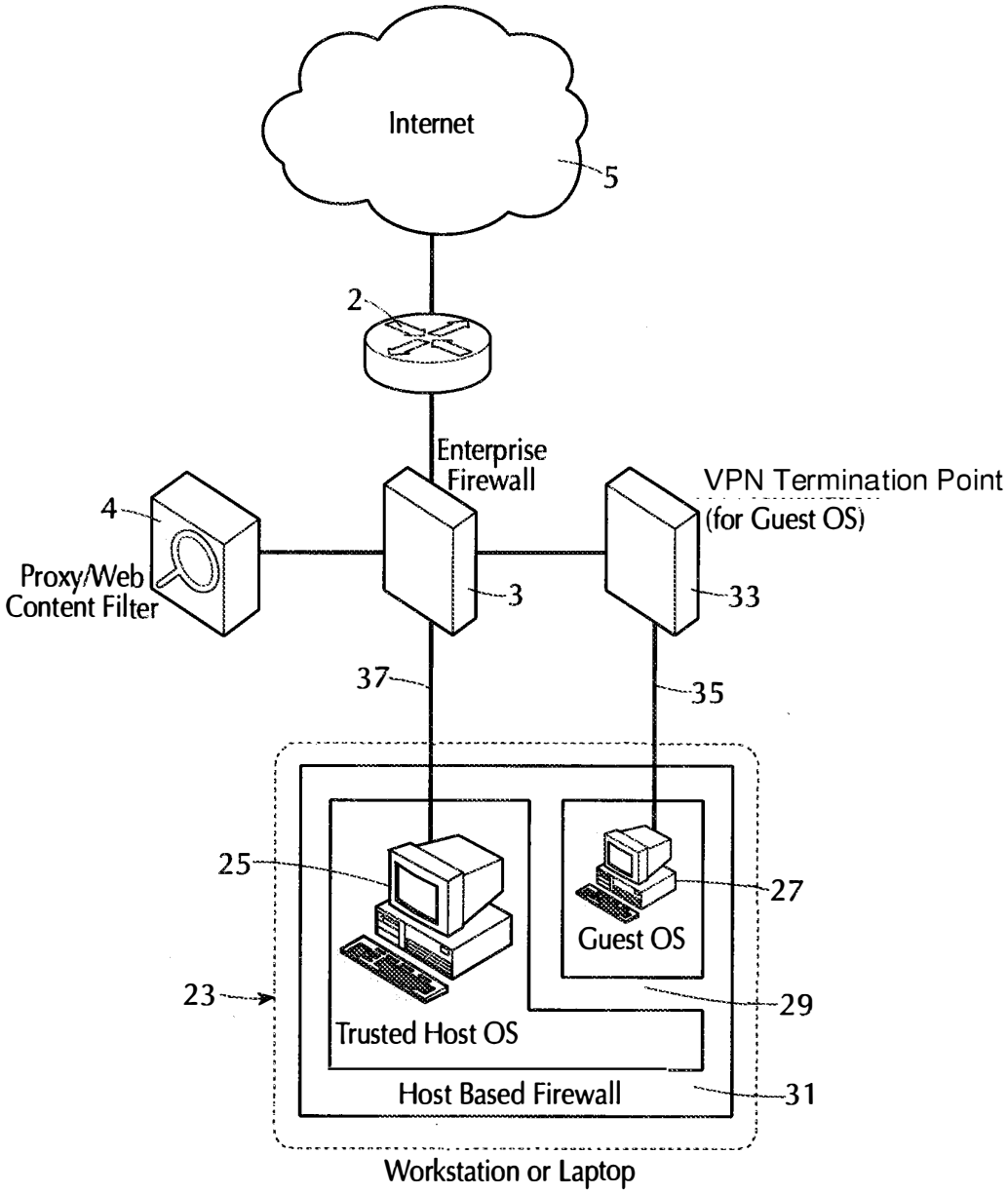

Internet
5
2
Enterprise
Firewall
VPN Termination Point
(for Guest OS)
4
Proxy/Web
Content Filter
3
33
37
35
25
27
Guest OS
23
29
Trusted Host OS
Host Based Firewall
31
Workstation or Laptop

FIG. 2

Electronic Acknowledgement Receipt

EFS ID:	31947060
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:	15027
Filer:	Joseph R. Klinicki/Darleen Yacovone
Filer Authorized By:	Joseph R. Klinicki
Attorney Docket Number:	LCOM_ISO_US02
Receipt Date:	02-MAR-2018
Filing Date:	
Time Stamp:	16:45:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1880
RAM confirmation Number	030518INTEFSW00003050505519
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	Application Data Sheet	LCOM_ISO_US02_ADS_as_filed.pdf	112436 cbd826d2475b0359225c4a2c2f7b9cc3a26beae1	no	9
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
2	Power of Attorney	LCOM_ISO_US02_POA_as_filed.pdf	217808 c78f9e6948f61da4531baa9162d626f333653b04	no	2
Warnings:					
Information:					
3		LCOM_ISO_US02_Preliminary_Amendment_as_filed.pdf	90002 283f8a7a20f8977cd94476f96692bdc9e857beb1	yes	8

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Preliminary Amendment	1	1
Specification	2	2
Claims	3	7
Applicant Arguments/Remarks Made in an Amendment	8	8

Warnings:					
Information:					
4	Authorization for Extension of Time all replies	LCOM_ISO_US02_EOT_Authorization_as_filed.pdf	68066 97ce67723922f27c950755e7fad02f57aac2b419	no	1
Warnings:					
Information:					

5	Miscellaneous Incoming Letter	LCOM_ISO_US02_Communication_Pursuant_to_37CFR155h_as_filed.pdf	76714 93c3c276310d80d2368da24b3be4e9a40a94c7a7	no	1
Warnings:					
Information:					
6		LCOM_ISO_US02_Specification_as_filed.pdf	1393535 9a33e1c0490e49707be7d3bd2f1accab0c9628c5	yes	29
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	20	
	Claims		21	27	
	Abstract		28	29	
Warnings:					
Information:					
7	Drawings-only black and white line drawings	LCOM_ISO_US02_Drawings_as_filed.pdf	52622 637ee5bd17d8cc3d403b0717acac02c9a3bf70d3	no	2
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	36828 f791391b733c97a109d6bdf79541fca17ffa6988	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2048011		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

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

Application Number	Not Yet Assigned
Filing Date	Herewith
First Named Inventor	Robert B. Hoy
Title	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	LCOM_ISO_US02

SIGNATURE of Applicant or Patent Practitioner

Signature	/Joseph R. Klinicki/	Date (Optional)	2018-03-02
Name	Jospeh R. Klinicki	Registration Number	68,505
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

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

☑ *Total of 1 forms are submitted.

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

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

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

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

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

Application Number	Filing Date

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

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 15027

OR

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

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

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

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

L3 Technologies, Inc.

☐ Inventor or Joint Inventor (title not required below)

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

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

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

SIGNATURE of Applicant for Patent

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

Signature		Date (Optional)	7-27-17
Name	Donald L. Letizia		
Title	VP, General Counsel CSG		

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

☑ Total of 1 forms are submitted.

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

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

DOCKET NO.: LCOM_ISO_US02 **PATENT**
Application No.: Not Yet Assigned

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **L3 TECHNOLOGIES, INC.**	**Confirmation No.: Not Yet Assigned**
Application No.: Not Yet Assigned	**Group Art Unit: Not Yet Assigned**
Filing Date: Herewith	**Examiner: Not Yet Assigned**

For: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

VIA EFS

Sir/Madam:

COMMUNICATION PURSUANT TO 37 CFR § 1.55(h)
STATEMENT OF SUBMISSION OF
CERTIFIED PRIORITY DOCUMENT IN PARENT PATENT APPLICATION

The present application for patent is a continuation of U.S. Patent Application No. 13/981,896, filed July 29, 2013, which is a National Stage Entry under 35 U.S.C. § 371 of Patent Cooperation Treaty Application No. PCT/US2012/023027, filed January 27, 2012, which claims priority from Application No. 61/436,932, filed January 27, 2011.

Applicant respectfully affirms that a certified copy of the priority document for Patent Application No. 61/436,932 was electronically retrieved by the USPTO in the corresponding parent patent application (U.S. Patent Application No. 13/981,896) on July 25, 2013 (and acknowledged by the Examiner in the Non-Final Rejection mailed February 2, 2015). Accordingly, Applicant has satisfied claim for priority in the present application for patent pursuant to 37 CFR § 1.55(h).

Date: March 2, 2018

/Joseph R. Klinicki/
Joseph R. Klinicki
Registration No. 68,505

Condo Roccia Koptiw LLP
1800 JFK Blvd., Suite 1700
Philadelphia, PA 19103
Telephone: (215) 558-5727
Facsimile: (215) 558-5676

REMARKS

Claims 28-47 will be pending in the application upon entry of the foregoing amendments. No claims have been amended. Claims 1-27 have been canceled. Claims 28-47 have been added. Support for the amendments can be found throughout the specification such as at pp. 10-19 of the as-filed specification, for example.

The specification has been amended to update the related applications.

No new matter has been added.

Conclusion

Applicants respectfully request that the foregoing amendments be entered, and that the present application be afforded substantive examination.

Date: March 2, 2018

/Joseph R. Klinicki/
Joseph R. Klinicki
Registration No. 68,505

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:	
Filing Date:	
Title of Invention:	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS
First Named Inventor/Applicant Name:	Robert B. Hoy
Filer:	Joseph R. Klinicki/Darleen Yacovone
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:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	1051	1	160	160
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1880**

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/910,734	Filing Date 03/02/2018	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	03/02/2018	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x $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**

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

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

LIE
SHERRY DAVIS

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/910,734	03/02/2018	2447	1880	LCOM_ISO_US02	20	2

CONFIRMATION NO. 2365

FILING RECEIPT

15027
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

OC000000093388862

Date Mailed: 03/28/2018

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

Inventor(s)

Robert B. Hoy, Sewell, NJ;
Mark Fenkner, Marlton, NJ;
Sean W. Farren, Newburyport, MA;

Applicant(s)

L3 Technologies, Inc., New York, NY;

Assignment For Published Patent Application

L3 Technologies, Inc., New York, NY

Power of Attorney: The patent practitioners associated with Customer Number 15027

Domestic Priority data as claimed by applicant

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

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 03/28/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/910,734**

Projected Publication Date: 07/05/2018

Non-Publication Request: No

Early Publication Request: No

Title

INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

Preliminary Class

709

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Espacenet

Bibliographic data: RU2406138 (C1) — 2010-12-10

SECURITY SYSTEM FOR VIRTUAL COMPUTER SYTEM

Inventor(s): ANDREEV STANISLAV VALER EVICH [RU]; DRAGAL CHUK VLADISLAV KONSTANTINOVICH [RU]; POPOV EVGENIJ ALEKSANDROVICH [RU] ± (Андреев Станислав Валерьевич (RU), ; Драгальчук Владислав Константинович (RU), ; Попов Евгений Александрович (RU))

Applicant(s): SAMSUNG ELECTRONICS CO LTD [KR] ± (KORPORATSIJA "SAMSUNG EHLEKTRONIKS KO., LTD.")

Classification: **- international:** *G06F12/08; G06F21/20*
- cooperative:

Application number: RU20090123225 20090618

Priority number(s): RU20090123225 20090618

Abstract of RU2406138 (C1)

FIELD: information technology. ^ SUBSTANCE: security system for a virtual computer system having a hardware part connected to at least one virtual machine through a virtual machine monitor which has a security policy control module, connected to a security subsystem having connected adjustment module and at least one security module connected to the virtual machine. ^ EFFECT: high efficiency and short response time. ^ 3 dwg

Ex.1002
CISCO SYSTEMS, INC. / Page 64 of 517

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION RU2406138

SYSTEM OF SECURITY OF THE VIRTUALIZED COMPUTER SYSTEM

The invention relates to the security of computer systems, namely, to the security systems of virtualized computer systems, and can be used in computer devices of various types with different architectural and operating systems that support virtualization capabilities.

The approach to virtualization capabilities associated with a virtual machine monitor (VMM) is in fact a typical way to create multiple virtual machines on a single real hardware platform. A virtual machine monitor is a computer program that performs full or partial monitoring of the resources of a real computer system. It provides an isolated environment by virtualizing hardware resource data. A virtualized environment is called a virtual machine (VM). A virtual machine can access virtual resources. Attempts to access virtual resources for virtual machines are controlled by the security subsystem. At the same time, from the point of view of the security subsystem, the virtual machine is the subject of the operation of circulation, and the resource to which it refers, the object. The security subsystem contains several (one or more) different elements, called security modules. When a virtual machine monitor organizes access to system resources, security modules decide to access subjects to objects based on the loaded security policy.

The security subsystem receives these decisions in a certain sequence and takes the final decision on their basis. In existing virtualization systems, the security module interrogation sequence is hard-coded. The performance aspect is not taken into account, or it is determined empirically in determining this sequence. Since decisions can be made very often and the sequence of interrogation of security modules may not be optimal, this can lead to a significant deterioration in the system's performance: a reduction in overall performance and response time.

The Xen virtualization system with the sHype security subsystem, developed by IBM, is well known (cf. Research Report RC23629: R.Sailer, T.Jaeger, E.Valdez, R.Perez, S.Berger, JL Griffin, L. van Doorn. Building a MAC-based Security Architecture for the Xen Opensource Hypervisor [1] and the Research Report RC23511: R.Sailer, E.Valdez, T.Jaeger, R.Perez, L. van Doorn, JLGriffin, S.Berger: sHype: Secure Hypervisor Approach to Trusted Virtualized Systems [2]). The sHype architecture (IBM) supports the implementation of various security modules (Chinese Wall, Biba, Bell-LaPadula, etc.).

The closest to the claimed invention is the security system of a virtualized computer system described in patent EP 2,037,657 [3], comprising a hardware associated with at least one virtual machine via a virtual machine monitor, wherein the virtual machine is configured to forward an access request to a virtual machine monitor configured to process the access request. This system was chosen as a prototype of the claimed invention.

The architecture of the analog and prototype systems described above assumes that the sequence of obtaining solutions from the security modules is based on the required security and is hard-coded. The performance aspect is not taken into account or it is determined empirically, which may not correspond to the real state. In systems with this architecture, overall system performance and system response time may deteriorate, especially if several complex security modules are used. In addition, this architecture does not provide functionality for recording events that occur in the security system.

The aim of the claimed invention is to create a security system for a virtualized computer system with increased performance and reduced response time.

The task is solved by creating an optimized sequence of polling the security modules and interrogating the modules in this sequence, and all modules are not required to be polled, if, after polling some modules, the information received is sufficient to make a decision. In addition, the subsystem of security added the ability to register events occurring in it. Event logging functions facilitate the administration of the security subsystem.

The technical result is achieved by creating a security system of a virtualized computer system comprising a hardware associated with at least one virtual machine through a virtual machine monitor that includes a security policy management

module connected to a security subsystem comprising a tuning module connected to each other and, at least one security module connected to the virtual machine, wherein the virtual machine is configured to forward the request access to the virtual machine monitor configured to process the access request, wherein the security subsystem is configured to interrogate the security modules, obtain permission from them and, based on the received decisions on the admission of the final approval decision, and the tuning module is executed with the ability to implement the function to configure the collection of information on the number of polls of each security module and the time spent on each of the polls, and with the possibility of determining on Nowe information collected optimal sequence poll security modules, in which often caused by modules and on which little time is wasted, causing one of the first.

For a better understanding of the claimed invention, a detailed description thereof will now be given with the corresponding drawings.

1. General scheme of the security system of the virtualized computer system according to the invention.

Fig. 2. A detailed diagram of the security system of the virtualized computer system according to the invention.

FIG. 3. The algorithm of the security system operation of the virtualized computer system according to the invention.

Let us consider the principle of functioning of the claimed invention. The claimed security system of the virtualized computer system (FIGS. 1 to 3) comprises a hardware part 1 associated with at least one virtual machine 2 via a virtual machine monitor 3 that includes a policy management module 4 connected to a security subsystem 5 comprising connected to each other by the tuning module 6 and at least one security module 7 connected to the virtual machine 2. The tuning module 6 provides functions for setting up and recording events. The functions of both types can be independently activated or deactivated by the security policy management module 4. The configuration functions have several modes.

Disabled - the security subsystem 5 operates in the normal mode (as if there were no configuration functions in the system).

Enabled - the security subsystem 5 constantly performs self-tuning (described later in this section).

Automatic mode - self-tuning of the subsystem 5 is initially enabled. The tuning module 6 checks the overhead for performing self-tuning. If the overhead of self-tuning exceeds its benefit (that is, determine the appropriateness of using self-tuning), self-tuning is turned off altogether or for a certain period of time.

For each access request, security modules 7 return an access decision. When the building function is enabled, the tuning module 6 collects information about the access decision requests. For each returned access decision, this information contains the number of polls of the security modules and the time spent by each module to determine its solution. Then, on request or after a certain time interval (i.e., periodically), the tuning module determines the optimal polling sequence of the security modules 7, which has the minimum expected execution time. Thus, the frequently called security modules 7 and modules, for which time is wasted, will be called among the first in the security module polling sequence. At the same time, restrictions on the permutation of security modules 7 in the polling sequence can be imposed.

The event logging functions of the security subsystem 5 can be turned on or off depending on the needs. This makes it possible to collect some information: subjects, objects, module solutions and final solutions. This information can be used for profiling and tracing the security subsystem, as well as for determining the correct configuration of the security subsystem and its verification.

Let us consider a preferred embodiment of the claimed invention. The virtualization system (FIG. 1) is a set of virtual machines 2 operating on any equipment with any architecture 1 and in any operating system. Each virtual machine 2 is independent and protected from the rest. The virtual machine monitor 3 ensures that this set of virtual machines 2 works correctly. All security information for virtual machines 2 and other resources is located inside the virtual machine monitor 3 and is protected from virtual machines 2.

Each virtual machine 2 can access various objects (virtual resources) that correspond to the real resources of the hardware part 1 of the system. When the virtual machine 2 tries to access the object, the access request is sent to the security subsystem 5 of the virtual machine monitor 3 (FIG. 2). The security subsystem 5 polls the security modules 7 and makes the final decision. Interrogation of all security modules 7 in a certain sequence may not be required - the final decision is available from the moment when the information received from the interrogated security modules 7 becomes sufficient to make a final decision.

Security subsystem 5 contains a configuration module 6 that performs setup functions (for self-tuning of the security subsystem) and event logging functions (for profiling / tracing the security subsystem). The functions of both types can be independently activated or deactivated by the policy management module.

For each access request, security modules 7 return an access decision. When the tuning functions are turned on, the tuning module 6 collects information about the access decision requests. For each returned access decision, this information contains the number of polls of the security modules 7 and the time taken by each module to generate the solution. Then, on demand or after a time interval (i.e., periodically), the tuning module determines the optimal polling sequence of the security modules 7, which has the minimum expected execution time. Thus, the frequently called modules 7 and the modules 7, which are spent very little time, will be interrogated among the first in the sequence of polling the security modules. At the same time, restrictions on the permutation of security modules 7 in the polling sequence can be imposed.

Thus, tuning functions increase the performance of the security subsystem.

Ex.1002
CISCO SYSTEMS, INC. / Page 66 of 517

If the registration of events is activated, it enables you to collect information: subjects, objects, module solutions and final decisions. This information can be used for profiling and tracing the security subsystem, and can also help in creating the correct configuration of the security subsystem.

The proposed system provides high performance of the security subsystem. In addition, it offers additional functionality - the ability to log events of the security subsystem. This information can be very useful for properly configuring the security subsystem in a virtualization system.

While the foregoing embodiment has been set forth to illustrate the present invention, it will be appreciated by those skilled in the art that various modifications, additions and substitutions are possible without departing from the scope and spirit of the present invention disclosed in the appended claims.

Ex.1002
CISCO SYSTEMS, INC. / Page 67 of 517

Europäisches Patentamt
European Patent Office
Office européen des brevets

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS RU2406138

A security system of a virtualized computer system comprising a hardware associated with at least one virtual machine through a virtual machine monitor that includes a security policy management module connected to a security subsystem comprising a connected setup module and at least one a security module coupled to the virtual machine, wherein the virtual machine is configured to direct the access request to the virtual machine monitor configured with the ability to process an access request, while the security subsystem is configured to interrogate security modules, obtain permission from them and, on the basis of decisions obtained, allow the final approval decision, and the configuration module is configured to: configure information gathering the number of polls of each security module and the time spent on each of the surveys, and the ability to determine, on the basis of the information collected, the optimal follower awn poll security modules, in which often caused by modules and on which little time is wasted, causing one of the first.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 406 138** (13) **C1**

(51) МПК
G06F 21/20 (2006.01)
G06F 12/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2009123225/08, 18.06.2009**

(24) Дата начала отсчета срока действия патента:
18.06.2009

(45) Опубликовано: **10.12.2010** Бюл. № **34**

(56) Список документов, цитированных в отчете о поиске: **RU 2007137570 A, 20.04.2009. US 2009133097 A1, 21.05.2009. CN 101425027 A, 06.05.2009. CN 101414913 A, 22.04.2009.**

Адрес для переписки:
119331, Москва, а/я 88, В.Н.Рослову

(72) Автор(ы):
Андреев Станислав Валерьевич (RU),
Драгальчук Владислав Константинович (RU),
Попов Евгений Александрович (RU)

(73) Патентообладатель(и):
Корпорация "САМСУНГ ЭЛЕКТРОНИКС Ко., Лтд." (KR)

(54) СИСТЕМА БЕЗОПАСНОСТИ ВИРТУАЛИЗОВАННОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ

(57) Реферат:

Изобретение относится к области безопасности компьютерных систем, а именно к системам безопасности виртуализованных компьютерных систем. Техническим результатом является высокая производительность и уменьшение времени отклика. Система безопасности виртуализованной компьютерной системы содержит аппаратную часть, связанную с, по меньшей мере, одной виртуальной машиной через монитор виртуальной машины, который содержит модуль управления политиками безопасности, соединенный с подсистемой безопасности, содержащей соединенные между собой настроечный модуль и, по меньшей мере, один модуль безопасности, соединенный с виртуальной машиной. 3 ил.

RU 2406138 C1

RU 2406138 C1

Ex.1002
CISCO SYSTEMS, INC. / Page 69 of 517



Фиг. 1

RU 2406138 C1

RU 2406138 C1

Ex.1002
CISCO SYSTEMS, INC. / Page 70 of 517

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 406 138** (13) **C1**

(51) Int. Cl.
G06F 21/20 (2006.01)
G06F 12/08 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2009123225/08, 18.06.2009**

(24) Effective date for property rights:
18.06.2009

(45) Date of publication: **10.12.2010 Bull. 34**

Mail address:
119331, Moskva, a/ja 88, V.N.Roslovu

(72) Inventor(s):
Andreev Stanislav Valer'evich (RU),
Dragal'chuk Vladislav Konstantinovich (RU),
Popov Evgenij Aleksandrovich (RU)

(73) Proprietor(s):
Korporatsija "SAMSUNG EhLEKTRONIKS Ko., Ltd." (KR)

(54) SECURITY SYSTEM FOR VIRTUAL COMPUTER SYTEM

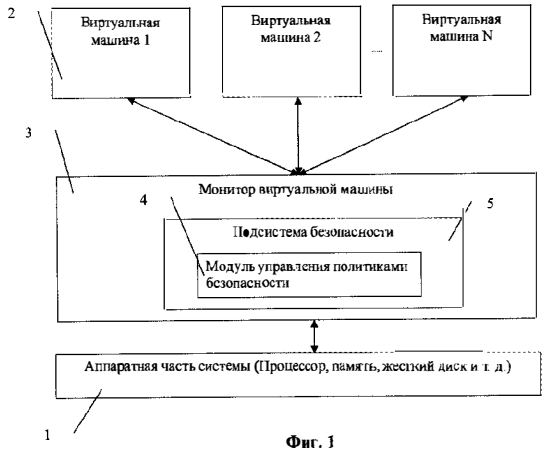
(57) Abstract:

FIELD: information technology.

SUBSTANCE: security system for a virtual computer system having a hardware part connected to at least one virtual machine through a virtual machine monitor which has a security policy control module, connected to a security subsystem having connected adjustment module and at least one security module connected to the virtual machine.

EFFECT: high efficiency and short response time.

3 dwg



Фиг. 1

RU 2406138 C1

RU 2406138 C1

Ex.1002
CISCO SYSTEMS, INC. / Page 71 of 517

Изобретение относится к области безопасности компьютерных систем, а именно к системам безопасности виртуализованных компьютерных систем, и может применяться в компьютерных устройствах различного типа с разными архитектурными и операционными системами, которые поддерживают возможности виртуализации.

Подход к возможностям виртуализации, связанный с монитором виртуальной машины (VMM - virtual machine monitor), фактически является типичным путем для создания нескольких виртуальных машин на единой реальной аппаратной платформе. Монитор виртуальной машины - это компьютерная программа, которая осуществляет полный или частичный контроль ресурсов реальной компьютерной системы. Она предоставляет изолированное окружение путем виртуализации данных аппаратных ресурсов. Виртуализованное окружение называется виртуальной машиной (VM - virtual machine). Виртуальная машина может обращаться к виртуальным ресурсам. Попытки обращения виртуальных машин к виртуальным ресурсам контролируются подсистемой безопасности. При этом, с точки зрения подсистемы безопасности, виртуальная машина является субъектом операции обращения, а ресурс, к которому она обращается, объектом. Подсистема безопасности содержит несколько (один или более) различных элементов, называемых модулями безопасности. Когда монитор виртуальной машины организовывает доступ к ресурсам системы, модули безопасности принимают решение о доступе субъектов к объектам на основе загруженной политики безопасности. Подсистема безопасности получает эти решения в определенной последовательности и принимает на их основе окончательное решение. В существующих системах виртуализации последовательность опроса модулей безопасности жестко закодирована. Аспект производительности не учитывается или она определяется эмпирически при определении данной последовательности. Поскольку решения могут приниматься очень часто и последовательность опроса модулей безопасности может быть неоптимальной, то это может привести к значительному ухудшению характеристик системы: уменьшению общей производительности и времени отклика.

Известна система виртуализации Xen с sHype подсистемой безопасности, разработанной фирмой IBM (см. Research Report RC23629: R.Sailer, T.Jaeger, E.Valdez, R.Perez, S.Berger, J.L Griffin, L. van Doorn: Building a MAC-based Security Architecture for the Xen Opensource Hypervisor [1] и Research Report RC23511: R.Sailer, E.Valdez, T.Jaeger, R.Perez, L. van Doorn, J.L.Griffin, S.Berger: sHype: Secure Hypervisor Approach to Trusted Virtualized Systems [2]). Архитектура sHype (фирмы IBM) поддерживает реализацию различных модулей безопасности (Chinese Wall, Biba, Bell-LaPadula и т.д.).

Наиболее близкой к заявленному изобретению является система безопасности виртуализованной компьютерной системы, описанная в патенте EP 2037657 [3], содержащая аппаратную часть, связанную, по меньшей, с одной виртуальной машиной через монитор виртуальной машины, при этом виртуальная машина выполнена с возможностью направления запроса доступа в монитор виртуальной машины, выполненный с возможностью обработки запроса доступа. Данная система выбрана в качестве прототипа заявленного изобретения.

Описанная выше архитектура систем аналога и прототипа предполагает, что последовательность получения решений от модулей безопасности основана на требуемой безопасности и жестко закодирована. Аспект производительности не учитывается или она определяется эмпирически, что может не соответствовать реальному состоянию. В системах с такой архитектурой может произойти ухудшение

Ex.1002
CISCO SYSTEMS, INC. / Page 72 of 517

общей производительности системы и времени отклика системы, особенно если используется несколько сложных модулей безопасности. Кроме того, данная архитектура не обеспечивает функциональности для регистрации событий, происходящих в системе безопасности.

Задачей заявленного изобретения является создание системы безопасности виртуализованной компьютерной системы с увеличенной производительностью и уменьшенным временем отклика.

Поставленная задача решена за счет формирования оптимизированной последовательности опроса модулей безопасности и опроса модулей в данной последовательности, при этом опрос всех модулей не требуется, если после опроса некоторых модулей полученной информации достаточно для принятия решения. Кроме того, в подсистему безопасности добавлена возможность регистрации происходящих в ней событий. Функции регистрации событий облегчают администрирование подсистемы безопасности.

Технический результат достигается благодаря созданию системы безопасности виртуализованной компьютерной системы, содержащей аппаратную часть, связанную с, по меньшей мере, одной виртуальной машиной через монитор виртуальной машины, который содержит модуль управления политиками безопасности, соединенный с подсистемой безопасности, содержащей соединенные между собой настроечный модуль и, по меньшей мере, один модуль безопасности, соединенный с виртуальной машиной, причем виртуальная машина выполнена с возможностью направления запроса доступа в монитор виртуальной машины, выполненный с возможностью обработки запроса доступа, при этом подсистема безопасности выполнена с возможностью опроса модулей безопасности, получения от них решений о допуске и с возможностью принятия на основе полученных решений о допуске окончательного решения о допуске, а настроечный модуль выполнен с возможностью реализации функции настройки сбора информации о количестве опросов каждого модуля безопасности и времени, израсходованном на каждый из опросов, и с возможностью определения на основе собранной информации оптимальной последовательности опроса модулей безопасности, при которой часто вызываемые модули и модули, на которые тратится мало времени, вызывают в числе первых.

Для лучшего понимания заявленного изобретения далее приводится его подробное описание с соответствующими чертежами.

Фиг.1. Общая схема системы безопасности виртуализованной компьютерной системы согласно изобретению.

Фиг.2. Подробная схема системы безопасности виртуализованной компьютерной системы согласно изобретению.

Фиг.3. Алгоритм работы системы безопасности виртуализованной компьютерной системы согласно изобретению.

Рассмотрим принцип функционирования заявленного изобретения. Заявленная система безопасности виртуализованной компьютерной системы (Фиг.1-3) содержит аппаратную часть 1, связанную с, по меньшей мере, одной виртуальной машиной 2 через монитор 3 виртуальной машины, который содержит модуль 4 управления политиками безопасности, соединенный с подсистемой 5 безопасности, содержащей соединенные между собой настроечный модуль 6 и, по меньшей мере, один модуль 7 безопасности, соединенный с виртуальной машиной 2. Настроечный модуль 6 обеспечивает функции настройки и регистрации событий. Функции обоих типов могут быть независимо активированы или деактивированы модулем 4 управления

Ex.1002
CISCO SYSTEMS, INC. / Page 73 of 517

политиками безопасности. Функции настройки имеют несколько режимов.

Выключен - подсистема 5 безопасности работает в обычном режиме (как если бы в системе не существовало функций настройки).

Включен - подсистема 5 безопасности постоянно выполняет самонастройку (описанную ниже в этом разделе).

Автоматический режим - изначально включена самонастройка подсистемы 5. Настроечный модуль 6 проверяет накладные расходы на выполнение самонастройки. Если накладные расходы самонастройки превышают ее выгоду (то есть определяют целесообразность использования самонастройки), то самонастройку выключают совсем или на определенный период времени.

На каждый запрос доступа модули 7 безопасности возвращают решение о доступе. Когда функция застройки включена, настроечный модуль 6 собирает информацию о запросах решения о доступе. Для каждого возвращенного решения о доступе данная информация содержит количество опросов модулей безопасности и время, израсходованное каждым модулем на выработку его решения. Затем по запросу или через определенный временной интервал (то есть периодически) настроечный модуль определяет оптимальную последовательность опроса модулей 7 безопасности, которая имеет минимальное ожидаемое время выполнения. Таким образом, часто вызываемые модули 7 безопасности и модули, на выполнение которых тратится мало времени, будут вызваны в числе первых в последовательности опроса модулей безопасности. При этом на перестановку модулей 7 безопасности в последовательности опроса могут накладываться определенные ограничения.

Функции регистрации событий подсистемы 5 безопасности могут быть включены или выключены в зависимости от потребностей. Это дает возможность собирать некоторую информацию: субъекты, объекты, решения модулей и окончательные решения. Данная информация может быть использована для профилирования и трассировки подсистемы безопасности, а также для определения правильной конфигурации подсистемы безопасности и ее проверки.

Рассмотрим предпочтительный вариант выполнения заявленного изобретения. Система виртуализации (Фиг.1) представляет собой набор виртуальных машин 2, работающих на любом оборудовании с любой архитектурой 1 и в любых операционных системах. Каждая виртуальная машина 2 независима и защищена от остальных. Монитор 3 виртуальной машины обеспечивает правильную работу данного набора виртуальных машин 2. Вся информация по безопасности, предназначенная для виртуальных машин 2 и других ресурсов, находится внутри монитора 3 виртуальной машины и защищена от виртуальных машин 2.

Каждая виртуальная машина 2 может получить доступ к различным объектам (виртуальным ресурсам), которые соответствуют реальным ресурсам аппаратной части 1 системы. Когда виртуальная машина 2 пытается получить доступ к объекту, запрос доступа посылают в подсистему 5 безопасности монитора 3 виртуальной машины (Фиг.2). Подсистема 5 безопасности опрашивает модули 7 безопасности и принимает окончательное решение. Опрос всех модулей 7 безопасности в определенной последовательности может не требоваться - окончательное решение доступно с того момента, когда информации, полученной от опрошенных модулей 7 безопасности, становится достаточно для принятия окончательного решения.

Подсистема 5 безопасности содержит настроечный модуль 6, который выполняет настроечные функции (для самонастройки подсистемы безопасности) и функции регистрации событий (для профилирования/трассировки подсистемы безопасности).

Ex.1002
CISCO SYSTEMS, INC. / Page 74 of 517

Функции обоих типов могут быть независимо активированы или деактивированы модулем управления политиками безопасности.

На каждый запрос доступа модули 7 безопасности возвращают решение о доступе. Когда настроечные функции включены, настроечный модуль 6 собирает информацию о запросах решения о доступе. Для каждого возвращенного решения о доступе эта информация содержит количество опросов модулей 7 безопасности и время, затраченное каждым модулем на выработку решения. Затем по запросу или через временной интервал (то есть периодически) настроечный модуль определяет оптимальную последовательность опроса модулей 7 безопасности, которая имеет минимальное ожидаемое время выполнения. Таким образом, часто вызываемые модули 7 и модули 7, на выполнение которых тратится мало времени, будут опрашиваться в числе первых в последовательности опроса модулей безопасности. При этом на перестановку модулей 7 безопасности в последовательности опроса могут накладываться определенные ограничения.

Таким образом, настроечные функции повышают производительность подсистемы безопасности.

Если регистрация событий активирована, то она дает возможность собирать информацию: субъекты, объекты, решения модулей и окончательные решения. Данная информация может быть использована для профилирования и трассировки подсистемы безопасности, а также может помочь при создании правильной конфигурации подсистемы безопасности.

Предложенная система обеспечивает высокую производительность подсистемы безопасности. Кроме того, она предлагает дополнительную функциональность - возможность регистрации событий подсистемы безопасности. Данная информация может быть очень полезна для правильного конфигурирования подсистемы безопасности в системе виртуализации.

Хотя указанный выше вариант выполнения изобретения был изложен с целью иллюстрации настоящего изобретения, специалистам ясно, что возможны разные модификации, добавления и замены, не выходящие из объема и смысла настоящего изобретения, раскрытого в прилагаемой формуле изобретения.

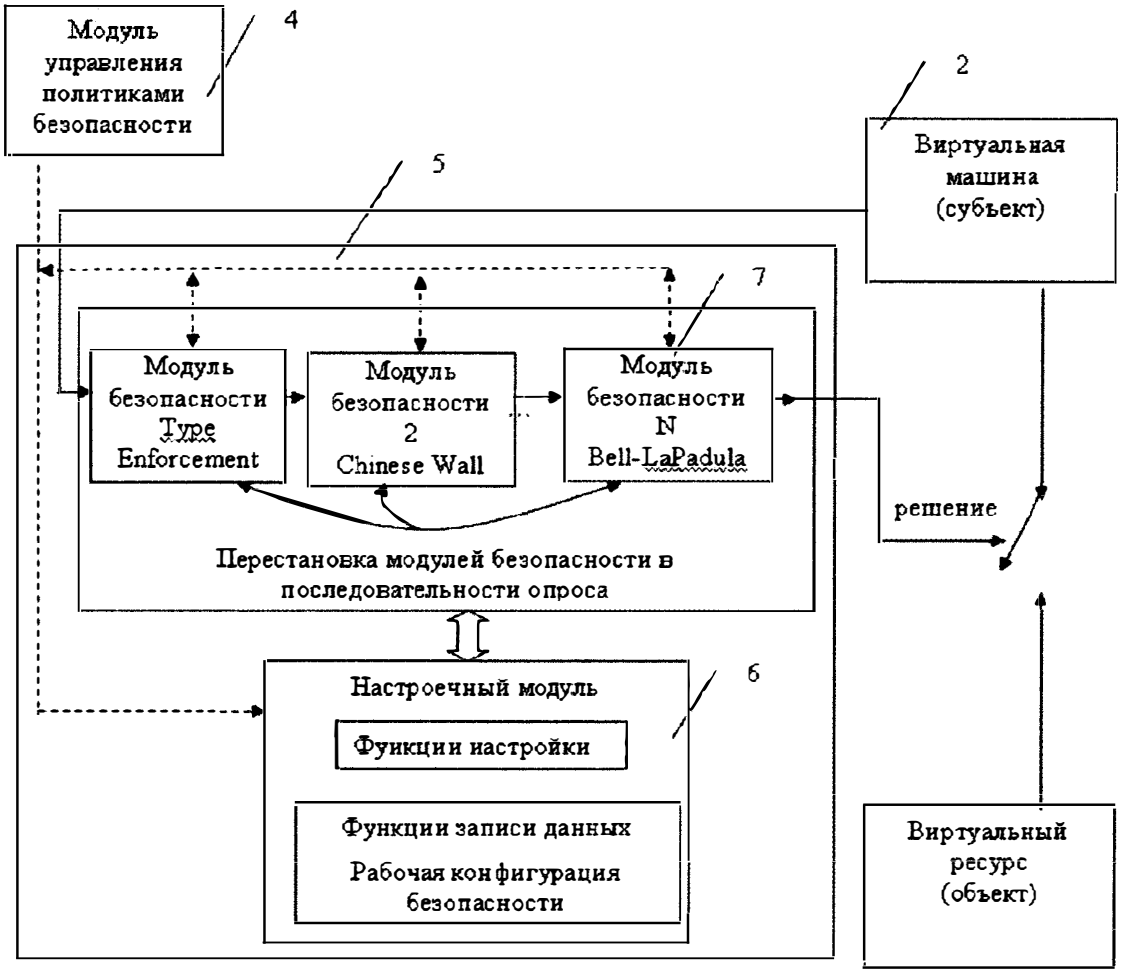
Формула изобретения

Система безопасности виртуализованной компьютерной системы, содержащая аппаратную часть, связанную с, по меньшей мере, одной виртуальной машиной через монитор виртуальной машины, который содержит модуль управления политиками безопасности, соединенный с подсистемой безопасности, содержащей соединенные между собой настроечный модуль и, по меньшей мере, один модуль безопасности, соединенный с виртуальной машиной, причем виртуальная машина выполнена с возможностью направления запроса доступа в монитор виртуальной машины, выполненный с возможностью обработки запроса доступа, при этом подсистема безопасности выполнена с возможностью опроса модулей безопасности, получения от них решений о допуске и с возможностью принятия на основе полученных решений о допуске окончательного решения о допуске, а настроечный модуль выполнен с возможностью реализации функции настройки: сбора информации о количестве опросов каждого модуля безопасности и времени, израсходованном на каждый из опросов, и с возможностью определения на основе собранной информации оптимальной последовательности опроса модулей безопасности, при которой часто вызываемые модули и модули, на которые тратится мало времени, вызывают в числе

Ex.1002
CISCO SYSTEMS, INC. / Page 75 of 517

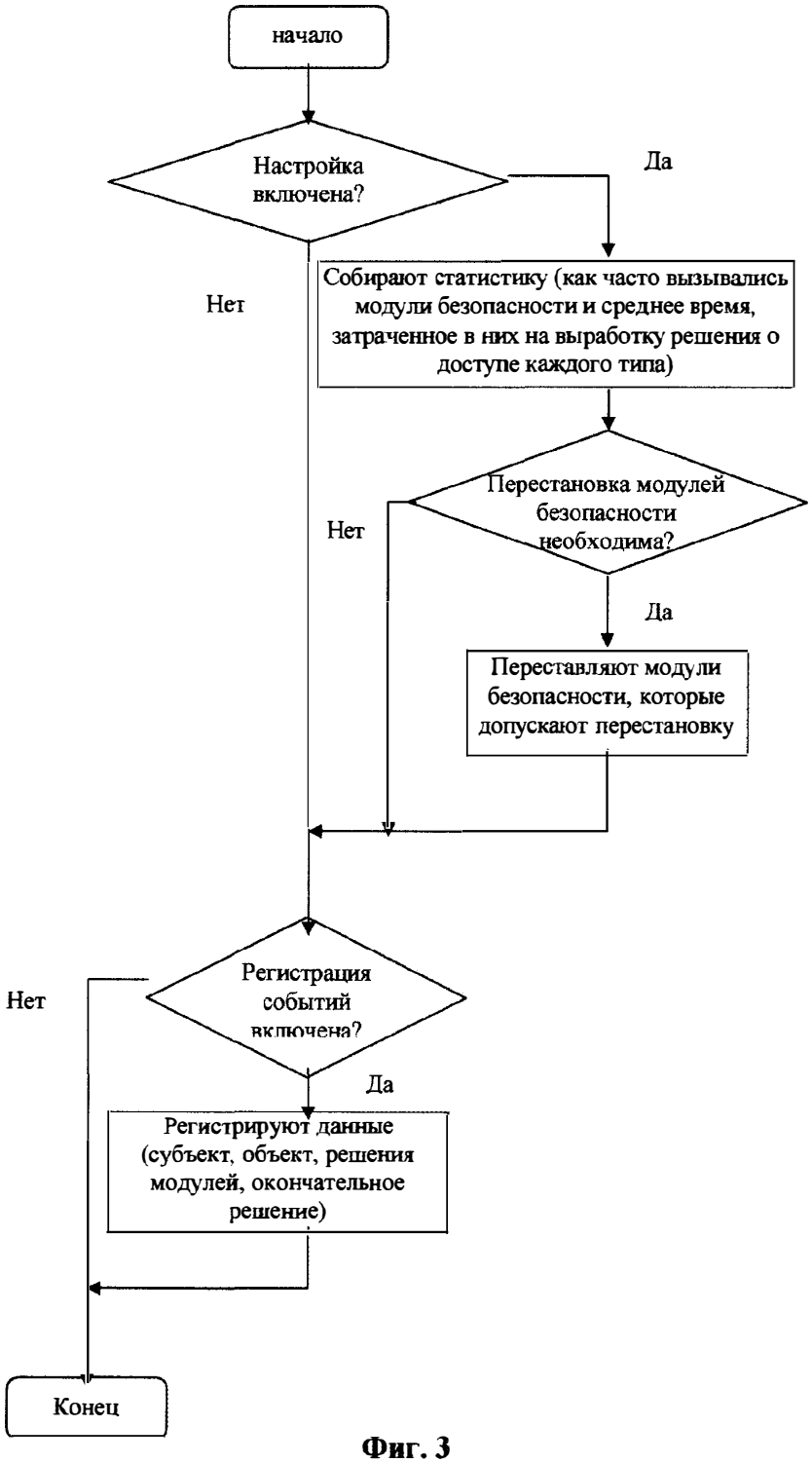
первых.

Ex.1002
CISCO SYSTEMS, INC. / Page 76 of 517



Фиг. 2

Ex.1002
CISCO SYSTEMS, INC. / Page 77 of 517



Фиг. 3

Ex.1002
CISCO SYSTEMS, INC. / Page 78 of 517

Substitute for 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application Number**	15/910,734
				Filing Date	March 2, 2018
				First Named Inventor	Robert B. Hoy
				Art Unit	2498
(use as many sheets as necessary)				**Examiner Name**	Not Yet Assigned
Sheet	1	of	2	**Attorney Docket Number**	LCOM_ISO_US02

U. S. PUBLICATION AND PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number – Kind Code (if known)	Publication or Grant Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1	7,478,330 B1	01-13-2009	Branson et al.
	2	7,698,442 B1	04-13-2010	Krishnamurthy et al.
	3	2002/0069369 A1	06-06-2002	Tremain, Geoffrey Donald
	4	2006/0070066 A1	03-30-2006	Grobman, Steven L.
	5	2007/0220187 A1	09-20-2007	Kates, Lawrence
	6	2007/0260873 A1	11-08-2007	Hatfalvi et al.
	7	2008/0028401 A1	01-31-2008	Geisinger, Nile Josiah
	8	2008/0201711 A1	08-21-2008	Amir Husain, Syed M.
	9	2008/0256536 A1	10-16-2008	Zhao et al.
	10	2009/0172781 A1	07-02-2009	Masuoka et al.
	11	2009/0328038 A1	12-31-2009	Yamada et al.
	12	2010/0138829 A1	06-03-2010	Hanquez et al.
	13	2010/0138830 A1	06-03-2010	Astete et al.
	14	2010/0223613 A1	09-02-2010	Schneider, James P.
	15	2010/0251329 A1	09-30-2010	Wei, Coach
	16	2012/0023593 A1	01-26-2012	Puder et al.

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code- Number - Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T
	17	RU 2406138 C1	12-10-2010	Samsung Electronics Co. Ltd.	X

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), Volume-issue Number(s), publisher, city and/or country where published.	T
	18	BARNET, MARK, "Praktikum Po Zaschite Seti Kompanii", Windows IT Pro/RE, November-December 2006, pp. 79-81	

Examiner Signature		**Date Considered**	

Substitute for 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application Number**	15/910,734
				Filing Date	March 2, 2018
				First Named Inventor	Robert B. Hoy
				Art Unit	2498
(use as many sheets as necessary)				**Examiner Name**	Not Yet Assigned
Sheet	2	of	2	**Attorney Docket Number**	LCOM_ISO_US02

U. S. PUBLICATION AND PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number – Kind Code (if known)	Publication or Grant Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	
	19	BURNETT, MARK, "How I Secured One Company's Network", Using Log Parser, Virtualization, and A Little Psychology, September 17, 2006, 4 pages			
	20	LAVERICK, MIKE, "Hypervisor Management and Optimization for Advanced Virtualization", E-book, Techtarget, November 2010, 13 pages			
	21	LI et al., "VSITE: A Scalable and Secure Architecture for Seamless L2 Enterprise Extension in the Cloud", 6th IEEE Workshop on Secure Network Protocols (NPSec), October 2010, 6 pages			
	22	REUBEN, JENNI SUSAN, "A Survey on Virtual Machine Security", TKK T-110.5290 Seminar on Network Security, October 11-12, 2007, 5 pages			
	23	VILLENEUVE, NART, "Command and Control in the Cloud", Malware Explorer, October 22, 2010, pp. 1-3			
	24	WIKIPEDIA, "Computer Network", Online Available at https://en.wikipedia.org/wiki/Computer_network , retrieved on December 2010, 6 pages			
	25	WIKIPEDIA, "Computer Security", Online Available at https://en.wikipedia.org/wiki/Computer_security , retrieved on December 2010, 11 pages			
	26	WIKIPEDIA, "Cyber Security Standards", Online Available at https://en.wikipedia.org/wiki/Cyber_security_standards , retrieved on December 2010, 5 pages			
	27	WIKIPEDIA, "HTTP Secure", Online Available at https://en.wikipedia.org/wiki/HTTPS , retrieved on December 2010, 6 pages			
	28	WIKIPEDIA, "Hypervisor", Online Available at https://en.wikipedia.org/wiki/Hypervisor , retrieved on December 2010, 6 pages			
	29	WIKIPEDIA, "Internet Protocol", Online Available at https://en.wikipedia.org/wiki/Internet_Protocol , retrieved on December 2010, 4 pages			
	30	WIKIPEDIA, "Multiprotocol Label Switching", Online Available at https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching , retrieved on December 2010, 8 pages			
	31	WIKIPEDIA, "Network Address Translation", Online Available at https://en.wikipedia.org/wiki/Network_address_translation , retrieved on December 2010, 9 pages			
	32	WIKIPEDIA, "Security-Focused Operating System", Online Available at https://en.wikipedia.org/wiki/Security-focused_operating_system , retrieved on December 2010, 4 pages			
	33	WIKIPEDIA, "Virtual Desktop", Available at https://en.wikipedia.org/wiki/Virtual_desktop , retrieved on December 2010, 6 pages			
	34	WIKIPEDIA, "Virtual Private Network", Online Available at https://en.wikipedia.org/wiki/Virtual_private_network , retrieved on December 2010, 7 pages			

Examiner Signature		**Date Considered**	

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/910,734	03/02/2018	Robert B. Hoy	LCOM_ISO_US02

CONFIRMATION NO. 2365

15027
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

INFORMAL NOTICE

OC000000098388863

Date Mailed: 03/28/2018

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Robert B. Hoy
  Mark Fenkner
  Sean W. Farren

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/cma/

Electronic Acknowledgement Receipt

EFS ID:	32187682
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:	15027
Filer:	Joseph R. Klinicki/melissa overline
Filer Authorized By:	Joseph R. Klinicki
Attorney Docket Number:	LCOM_ISO_US02
Receipt Date:	28-MAR-2018
Filing Date:	02-MAR-2018
Time Stamp:	17:44:18
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	Transmittal Letter	LCOM_ISO_US02_AS_FILED_IDS_TRANS.pdf	104548 3193a17972fa3793Scce97faeba05d2bc5a02e76	no	3

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	LCOM_ISO_US02_AS_FILED_IDS_1449.pdf	135142 af02335834e3a8531ea2c925b509d975157032b8	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	RU_2406138.pdf	2817442 36e9aceb5347e29864bcf7dda2f8ded2e742b163	no	15
Warnings:					
Information:					
			Total Files Size (in bytes):	3057132	

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.

DOCKET NO.: LCOM_ISO_US02 **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 02, 2018 **Examiner: Not Yet Assigned**

For: INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

Filed Via EFS

INFORMATION DISCLOSURE STATEMENT

Pursuant to 37 CFR § 1.56 and in accordance with 37 CFR §§ 1.97-1.98, information relating to the above-identified application is hereby disclosed. Inclusion of information in this statement is not to be construed as an admission that this information is material as that term is defined in 37 CFR § 1.56(b).

☒ **IDS Filed Under 37 CFR 1.97(b)**

In accordance with § 1.97(b), since this Information Disclosure Statement is being filed either within three months of the filing date of the above-identified application, within three months of the date of entry into the national stage of the above identified application as set forth in § 1.491, before the mailing date of a first Office Action on the merits of the above-identified application, or before the mailing date of a first Office Action after the filing of request for continued examination under § 1.114, no additional fee is required.

☐ **IDS filed Under 37 CFR 1.97(c)**

In accordance with § 1.97(c), this Information Disclosure Statement is being filed after the period set forth in § 1.97(b) above but before the mailing date of either a Final Action under § 1.116 or a Notice of Allowance under § 1.311, or before an action that otherwise closes prosecution in the application, therefore:

- ☐ Certification in Accordance with § 1.97(e) is attached; or
- ☐ The fee of **$240.00** as set forth in § 1.17(p) is attached.

☐ **IDS filed Under 37 CFR 1.97(d)**

In accordance with § 1.97(d), this Information Disclosure Statement is being filed after the mailing date of either a Final Action under § 1.113 or a Notice of Allowance under § 1.311 but before, or simultaneously with, the payment of the Issue Fee, therefore included are: Certification in Accordance with § 1.97(e); and the submission fee of **$240.00** as set forth in § 1.17(p).

CONTENT OF IDS PURSUANT TO 37 CFR 1.98

☒ Copies of reference numbers 01-16 listed on the attached Form PTO-1449 are not required to be submitted pursuant to 37 CFR § 1.98(a)(2)(ii).

☒ Copy of reference number 17 listed on the attached Form PTO-1449 is enclosed herewith.

☒ Copies of reference numbers 18-34 are not being submitted because they were previously cited by or submitted to the U.S. Patent and Trademark Office in patent application number 13/981,896, filed July 29, 2013 for which a claim for priority under 35 U.S.C. § 120 has been made in the instant application.

☐ The month of publication for reference numbers is not available. However, the year of publication for these references is sufficiently earlier than the effective US filing date and any foreign priority date so that the particular month of publication is not in issue pursuant to 37 CFR § 1.98(b).

REFERENCES IN A LANGUAGE OTHER THAN ENGLISH

☒ The following documents are not in the English language. Accordingly, a concise explanation of the relevance of the document was incorporated in the specification passages identified below, the document was identified in a foreign communication as identified below or an English language counterpart application has been provided as indicated below.

Foreign Language Document	Cite No.	Pages of Reference in Specification or Relevance of Document

RU 2406138 C1	17	Cited in International Search Report dated May 24, 2012, issued in related PCT Application No. PCT/US2012/023027

Foreign Language Document	Cite No.	English Language Counterpart	Cite No.

☐ **CERTIFICATION IN ACCORDANCE WITH § 1.97(e)**

I hereby certify that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this information disclosure statement.

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

Please charge any deficiency or credit any overpayment to Deposit Account No. 50-5519.

Date: March 28, 2018

/Joseph R. Klinicki/
Joseph R. Klinicki
Registration No. 68,505

CONDO ROCCIA KOPTIW LLP
1800 JFK BOULEVARD
SUITE 1700
PHILADELPHIA, PA 19103
Telephone: (215) 558-5740

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/910,734

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	660
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 460 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1720

APPLICATION AS AMENDED - PART II

AMENDMENT A

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

AMENDMENT B

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

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

Notice of References Cited	Application/Control No. 15/910,734	Applicant(s)/Patent Under Reexamination HOY ET AL.	
	Examiner WAYNE AN	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-				
	B	US-				
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	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	Reuben, Jenni Susan, "A Survey on Virtual Machine Security", TKK T-110.5290 Seminar on Network Security, October 11-12, 2007, 5 Pages
	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.

Substitute for 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	15/910,734
				Filing Date	March 2, 2018
				First Named Inventor	Robert B. Hoy
				Art Unit	2498
(use as many sheets as necessary)				Examiner Name	Not Yet Assigned
Sheet	1	of	2	Attorney Docket Number	LCOM_ISO_US02

U. S. PUBLICATION AND PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number – Number – Kind Code (if known)	Publication or Grant Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1	7,478,330 B1	01-13-2009	Branson et al.
	2	7,698,442 B1	04-13-2010	Krishnamurthy et al.
	3	2002/0069369 A1	06-06-2002	Tremain, Geoffrey Donald
	4	2006/0070066 A1	03-30-2006	Grobman, Steven L.
	5	2007/0220187 A1	09-20-2007	Kates, Lawrence
	6	2007/0260873 A1	11-08-2007	Hatfalvi et al.
	7	2008/0028401 A1	01-31-2008	Geisinger, Nile Josiah
	8	2008/0201711 A1	08-21-2008	Amir Husain, Syed M.
	9	2008/0256536 A1	10-16-2008	Zhao et al.
	10	2009/0172781 A1	07-02-2009	Masuoka et al.
	11	2009/0328038 A1	12-31-2009	Yamada et al.
	12	2010/0138829 A1	06-03-2010	Hanquez et al.
	13	2010/0138830 A1	06-03-2010	Astete et al.
	14	2010/0223613 A1	09-02-2010	Schneider, James P.
	15	2010/0251329 A1	09-30-2010	Wei, Coach
	16	2012/0023593 A1	01-26-2012	Puder et al.

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document – Country Code- Number - Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T
	17	RU 2406138 C1	12-10-2010	Samsung Electronics Co. Ltd.	X

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), Volume-issue Number(s), publisher, city and/or country where published.	T
	18	BARNET, MARK, "Praktikum Po Zaschite Seti Kompanii", Windows IT Pro/RE, November-December 2006, pp. 79-81	

Examiner Signature	/Wayne An/	Date Considered	4/16/2018

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /WA/

Substitute for 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application Number**	15/910,734
				Filing Date	March 2, 2018
				First Named Inventor	Robert B. Hoy
				Art Unit	2498
(use as many sheets as necessary)				**Examiner Name**	Not Yet Assigned
Sheet	2	of	2	**Attorney Docket Number**	LCOM_ISO_US02

U. S. PUBLICATION AND PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number – Kind Code (if known)	Publication or Grant Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	~~19~~	BURNETT, MARK, "How I Secured One Company's Network", Using Log Parser, Virtualization, and A Little Psychology, September 17, 2006, 4 pages		
	~~20~~	LAVERICK, MIKE, "Hypervisor Management and Optimization for Advanced Virtualization", E-book, Techtarget, November 2010, 13 pages		
	~~21~~	LI et al., "VSITE: A Scalable and Secure Architecture for Seamless L2 Enterprise Extension in the Cloud", 6th IEEE Workshop on Secure Network Protocols (NPSec), October 2010, 6 pages		
	~~22~~	REUBEN, JENNI SUSAN, "A Survey on Virtual Machine Security", TKK T-110.5290 Seminar on Network Security, October 11-12, 2007, 5 pages		
	~~23~~	VILLENEUVE, NART, "Command and Control in the Cloud", Malware Explorer, October ~~22, 2010, pp. 1-3~~		
	~~24~~	WIKIPEDIA, "Computer Network", Online Available at https://en.wikipedia.org/wiki/Computer_network , retrieved on December 2010, 6 pages		
	~~25~~	WIKIPEDIA, "Computer Security", Online Available at https://en.wikipedia.org/wiki/Computer_security , retrieved on December 2010, 11 pages		
	~~26~~	WIKIPEDIA, "Cyber Security Standards", Online Available at ~~https://en.wikipedia.org/wiki/Cyber_security_standards , retrieved on December 2010, 5~~ pages		
	~~27~~	WIKIPEDIA, "HTTP Secure", Online Available at https://en.wikipedia.org/wiki/HTTPS , retrieved on December 2010, 6 pages		
	~~28~~	WIKIPEDIA, "Hypervisor", Online Available at https://en.wikipedia.org/wiki/Hypervisor , retrieved on December 2010, 6 pages		
	~~29~~	WIKIPEDIA, "Internet Protocol", Online Available at https://en.wikipedia.org/wiki/Internet_Protocol , retrieved on December 2010, 4 pages		
	~~30~~	WIKIPEDIA, "Multiprotocol Label Switching", Online Available at ~~https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching , retrieved on December 2010,~~ 8 pages		
	~~31~~	WIKIPEDIA, "Network Address Translation", Online Available at ~~https://en.wikipedia.org/wiki/Network_address_translation , retrieved on December 2010, 9~~ pages		
	~~32~~	WIKIPEDIA, "Security-Focused Operating System", Online Available at ~~https://en.wikipedia.org/wiki/Security-focused_operating_system , retrieved on December~~ 2010, 4 pages		
	~~33~~	WIKIPEDIA, "Virtual Desktop", Available at https://en.wikipedia.org/wiki/Virtual_desktop , retrieved on December 2010, 6 pages		
	~~34~~	WIKIPEDIA, "Virtual Private Network", Online Available at ~~https://en.wikipedia.org/wiki/Virtual_private_network , retrieved on December 2010, 7~~ pages		

Examiner Signature	/Wayne An/	**Date Considered**	04/16/2018

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /WA/

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

15027 7590 06/05/2018
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

EXAMINER	
AN, WAYNE	

ART UNIT	PAPER NUMBER
2498	

MAIL DATE	DELIVERY MODE
06/05/2018	PAPER

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

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

Office Action Summary	Application No. 15/910,734	Applicant(s) HOY ET AL.	
	Examiner WAYNE AN	Art Unit 2498	AIA (First Inventor to File) Status No

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *3/2/2018.*

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

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

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

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

Disposition of Claims*

5)☒ Claim(s) *28-47* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *28-47* is/are rejected.

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

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

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

Application Papers

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

11)☒ The drawing(s) filed on *3/2/2018* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☒ All b)☐ Some** c)☐ None of the:

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

2.☒ Certified copies of the priority documents have been received in Application No. 13/981896.

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

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

Attachment(s)

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

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *3/28/2018.*

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

2. Claims 28-47 are pending for examination.

Information Disclosure Statement

3. The following Information Disclosure Statement(s) in the instant application submitted in compliance with the provisions of 37 CFR 1.97, and thus, have been fully considered:

a. IDS filed on 3/28/2018 is NOT compliant.

i. Examiner notes that none of the Non-Patent Literature documents listed were considered because Applicant failed to provide copies for Examiner's consideration.

Drawings

4. The submitted drawing filed on 3/2/2018, for the instant application is acceptable for examination purposes.

Claim Rejections - 35 USC § 103

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claim 28-47 rejected under 35 U.S.C. 103 as being unpatentable over Hatfalvi (US 2007/0260873), and in view of Reuben ("A Survey on Virtual Machine Security").

All references were cited in Applicant's IDS filed on 3/28/2018.

6. As per **claim 28**, Hatfalvi discloses a networked computer system (Fig. 2, 200 Protected Network) comprising:

a network (Fig. 1 and Fig. 2, external networks 150; [0026] external networks 150...provides its Internet-access services);

at least one computer system configured to connect to the network (Fig. 2, 210 protected computer(s) all of which are located inside their respective Protected Networks 100 and 200),

the computer system comprising a host system (Fig. 2, 210 protected computer) and a virtual system (Fig. 2, 220 SVM or special virtual machine); 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 ([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).

Hatfalvi does not disclose 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

However, Reuben discloses 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 (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…the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking…enough isolation should be provided; Examiner notes that isolating the host machines from the virtual computer will protect the host machines and the host machine would receive input (keystrokes) from a user in order to view and/or copy data from the VM)

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.

7. As per **claim 29**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input (Reuben, Part 1, Paragraph 1, virtual machines (VM) or guest machines…multiple operating systems to use the hardware of the physical machine is called a hypervisor; 4.3 VM monitoring from the host, it is more necessary to strictly protect the host machines…the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking…enough isolation should be provided).

8. As per **claim 30**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space (Reuben, 3 Background, Paragraph 8, every guest machines appears to be an independent computer; Fig. 1 each guest OS takes up a portion of the hardware and has to share computer resources with other guest OSes).

9. As per **claim 31**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system (Reuben, 4.3 Paragraph 2, the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking).

10. As per **claim 32**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the computer system is configured to: communicate with the one or more untrusted network destinations via a first communication connection, communicate with one or more trusted network destinations via a second 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 (Reuben, 4.3 Paragraph 2, the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking).

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),

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; implementing network isolation between the computer system and the network using a host-based 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; implementing network isolation between the computer system and the network using a host-based 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. 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, 8am-5pm 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.

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

/CATHERINE THIAW/
Primary Examiner, Art Unit 2493

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15910734	HOY ET AL.
	Examiner	Art Unit
	WAYNE AN	2498

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

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

CLAIM		DATE								
Final	Original	04/30/2018								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15910734	HOY ET AL.
	Examiner	Art Unit
	WAYNE AN	2498

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587	4/30/2018	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

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
L1	2	((("Hoy") near3 ("Robert") near3 ("B"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:08
L2	2	((("Fenkner") near3 ("Mark"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:19
L3	2	((("Farren") near3 ("Sean") near3 ("W"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:19
L4	24	("L3 Technologies").as.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 12:19
L5	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
L6	25032	(H04L63/0272,101; G06F9/45558; G06F21/52; G06F2009/45587).cpc.	US-PGPUB; USPAT; USOCR	OR	ON	2018/04/30 15:04

4/30/2018 4:53:27 PM
C:\Users\wan\Documents\EAST\Workspaces\15910734.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/910,734	03/02/2018	Robert B. Hoy	LCOM_ISO_US02

CONFIRMATION NO. 2365

15027
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

PUBLICATION NOTICE



Title:INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

Publication No.US-2018-0191684-A1
Publication Date:07/05/2018

NOTICE OF PUBLICATION OF APPLICATION

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

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

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
15/910,734		2498	73874

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 158266 on 10/17/2018 via Private PAIR in view of the certification copied below that authorized the change.

- Maintenance Fee Address

The address for Customer Number 158266 is:
158266
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Joseph R. Klinicki/
Name:	Joseph R. Klinicki
Registration Number:	68505

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
15/910,734		2498	73874

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 158266 on 10/17/2018 via Private PAIR in view of the certification copied below that authorized the change.

- Correspondence Address

The address for Customer Number 158266 is:
158266
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Joseph R. Klinicki/
Name:	Joseph R. Klinicki
Registration Number:	68505

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: Wayne An**

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 **June 5, 2018**, 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:	34479602
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:	Joseph R. Klinicki/MELISSA OVERLINE
Filer Authorized By:	Joseph R. Klinicki
Attorney Docket Number:	LCOM_ISO_US02
Receipt Date:	04-DEC-2018
Filing Date:	02-MAR-2018
Time Stamp:	14:42:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1400
RAM confirmation Number	120618INTEFSW14475600
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_Reply_to_NFOA_Dated_06_05_18.pdf	124847 1d6d30df43d2f286e541365ea7842d1782a4f12d	yes	5
	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	5	
Warnings:					
Information:					
2	Extension of Time	LCOM_ISO_US02_AS_FILED_EOT.pdf	132933 615960cde5898d85646f6134d916a889c667aff1	no	2
Warnings:					
Information:					
3	Oath or Declaration filed	LCOM_ISO_US02_AS_FILED_Declarations.pdf	841873 39cc8a534294a0aab5ba32725c903febc19ef9ac	no	2
Warnings:					
Information:					
4	Oath or Declaration filed	LCOM_ISO_US02_AS_FILED_Substitute_Statement_Hoy.pdf	2925170 9196fec96701d87a0792dfab434da76142dd08ce	no	2
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	31003 d6ac6595657e69f8d01c5d187bd97ae2ee788ab7	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	4055826

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.

Substitute Form for PTO/AIA/01

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

Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

As the below named inventor, I hereby declare that:

This declaration is directed to: ☐ The attached application, or

☒ United States application or PCT international application number 15/910,734

filed on March 2, 2018.

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

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

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

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Mark Fenkner Date: 7/16/19

Signature:

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional Substitute Form for PTO/SB/AIA01 for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14.

LCOM_ISO_US02

Substitute Form for PTO/AIA/01

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

Title of invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 15/910,734

filed on March 2, 2018

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

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

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

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Sean W. Farren Date: 6/4/18

Signature:

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

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14.

Doc code: Oath
Document Description: Oath or declaration filed

PTO/AIA/02 (07-13)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)

Title of Invention	INTERNET ISOLATION FOR AVOIDING INTERNET SECURITY THREATS

This statement is directed to:

☐ The attached application,

OR

☒ United States application or PCT international application number 15/910,734 filed on 03-02-2018.

LEGAL NAME of inventor to whom this substitute statement applies:

(*E.g.*, Given Name (first and middle (if any)) and Family Name or Surname)

Robert B. Hoy

Residence (except for a deceased or legally incapacitated inventor):

City	State	Country
Sewell	NJ	US

Mailing Address (except for a deceased or legally incapacitated inventor):

600 Third Avenue

City	State	Zip	Country
New York	NY	10016	US

I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.

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

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

Relationship to the inventor to whom this substitute statement applies:

- ☐ Legal Representative (for deceased or legally incapacitated inventor only),
- ☐ Assignee,
- ☒ Person to whom the inventor is under an obligation to assign,
- ☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or
- ☐ Joint Inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased,
- ☐ Inventor is under legal incapacity,
- ☐ Inventor cannot be found or reached after diligent effort, or
- ■ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ■ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

WARNING:

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

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

Name: Donald L. Letizia | Date (Optional):

Signature:

APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

If the applicant is a juristic entity, list the applicant name and the title of the signer:

Applicant Name: L3 Technologies, Inc.

Title of Person Executing This Substitute Statement: VP, General Counsel CSG

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City New York | State NY | Country US

Mailing Address of the signer (unless provided in a n application data sheet, PTO/AIA/14 or equivalent)

600 Third Avenue

City New York | State NY | Zip 10016 | Country US

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

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 An for participating in a telephonic interview with Applicant's undersigned representative on December 3, 2018. During the interview, the references cited in the Office Action and the pending claims were discussed. Although no formal agreement was reached, Examiner An indicated that claim 33 appeared to further prosecution, but that he would need to re-visit the references and perform an additional search.

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

The Office Action admits that Hatfalvi does not disclose "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," as independent claim 28 recites in part (Office Action, p. 4). Claim 38 recites similar subject matter. Instead, the Office Action relies on Reuben for allegedly teaching such subject matter.

However, such functionality for a local host-based firewall used on a computer system having a virtual system operating thereon is nowhere taught or suggested by Reuben. For at least this reason, the rejections to claims 28 and 38 under 35 U.S.C. § 103 should be withdrawn.

For example, Reuben 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. Simply stated, Reuben does not contemplate 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 ***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.

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. Neither Hatfalvi nor Reuben teach or suggest such subject matter.

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.

Rather, Hatfalvi generally discloses two embodiments. The first, related to FIG. 1, utilizes a browser module outside of a protected network to perform browsing on behalf of one or more computers utilizing a Browsing Client within the protected network (*See e.g.*, Hatfalvi, paragraphs [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, paragraph [0046]).

However, the system of Hatfalvi nowhere teaches or suggests that either 1) there may be communications to be sent by the protected computer system that arise from applications outside of the SVM, or 2) that some communications may be between resources on a local area network rather than the Internet. Moreover, there is absolutely no mention in Hatfalvi about use of **a host-based firewall** on the protected computer systems, let alone ***a host-based firewall*** that is configured to ***prevent lateral communication and movement of malware between the computer system and other devices on the 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 38.

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 38.

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, 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 An 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: December 4, 2018

/Joseph R. Klinicki/
Joseph R. Klinicki
Registration No. 68,505

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:	Joseph R. Klinicki/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($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
			Total in USD ($)	**1400**

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 03/19/2019

Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

EXAMINER	
AN, WAYNE	

ART UNIT	PAPER NUMBER
2498	

MAIL DATE	DELIVERY MODE
03/19/2019	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.

Office Action Summary	Application No. 15/910,734	Applicant(s) Hoy et al.	
	Examiner WAYNE AN	Art Unit 2498	AIA (FITF) Status No

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

Period for Reply

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

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

Status

1)☑ Responsive to communication(s) filed on 12/4/2018.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 28-47 is/are pending in the application.

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

6) ☐ Claim(s) ____ is/are allowed.

7) ☑ Claim(s) 28-47 is/are rejected.

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

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

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

Application Papers

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

11)☑ The drawing(s) filed on 3/2/2018 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Response to Arguments

2. Applicant's argument, filed 12/4/2018, regarding the claims have been fully considered but they are not persuasive.

3. In the remarks, applicant argued the following:

a. Reuben cannot be said to teach or suggest 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. Such functionality for a local host-based firewall used on a computer system having a virtual system operating thereon is nowhere taught or suggested by Reuben. For at least this reason, the rejections to claims 28 and 38 under 35 U.S.C. § 103 should be withdrawn.

b. 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. Neither Hatfalvi nor Reuben teach or suggest such subject matter.

4. Examiner respectfully disagrees with applicant's arguments.

a. As to point a. above, Examiner thanks Applicant for clarifying the claim limitations in an interview conducted on December 3, 2018. After further search and consideration, Examiner believes that Hatfalvi does teach the limitations that the Applicant is arguing. In Hatfalvi's system, there is a protected computer that is utilized to comprise a browser module. The protected computer is further protected by using border and browser modules which can be integrated with the computer itself. Furthermore, host-based is a term that can be interpreted as being a part of the host but not necessarily inside the host and therefore under BRI, Hatfalvi teaches the host-based firewall that is claimed (See Hatfalvi [0021], [0024], [0025]).

b. As to point b. above, it is similar to point a. above where Hatfalvi teaches the firewall protecting the computers on network. It is also well known in the field of endeavor that a firewall is on a host computer in order to protect the host from any malicious computers on the same network (See Hatfalvi [0003], [0005], [0024], [0025], [0026]).

Claim Rejections - 35 USC § 103

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claim 28-47 rejected under 35 U.S.C. 103 as being unpatentable over Hatfalvi (US 2007/0260873), and in view of Reuben ("A Survey on Virtual Machine Security'').

All references were cited in Applicant's IDS filed on 3/28/2018.

6. As per **claim 28**, Hatfalvi discloses a networked computer system (Fig. 2, 200 Protected Network) comprising:

a network (Fig. 1 and Fig. 2, external networks 150; [0026] external networks 150...provides its Internet-access services);

at least one computer system configured to connect to the network (Fig. 2, 210 protected computer(s) all of which are located inside their respective Protected Networks 100 and 200),

the computer system comprising a host system (Fig. 2, 210 protected computer) and a virtual system (Fig. 2, 220 SVM or special virtual machine) and a host-based firewall executed on the computer system is configured to implement network isolation between the computer system and the network ([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); 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 ([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).

Hatfalvi does not disclose 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,

However, Reuben discloses 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 (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…the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking…enough isolation should be provided; Examiner notes that isolating the host machines from the virtual computer will protect the host machines and the host machine would receive input (keystrokes) from a user in order to view and/or copy data from the VM)

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.

7. As per **claim 29**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the internal firewall is configured to prevent data from being communicated between the virtual system and the host system without an explicit user input (Reuben, Part 1, Paragraph 1, virtual machines (VM) or guest machines…multiple operating systems to use the hardware of the physical machine is called a hypervisor;

4.3 VM monitoring from the host, it is more necessary to strictly protect the host machines…the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking…enough isolation should be provided).

8. As per **claim 30**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the host system is configured to store data in a host memory space and the virtual system is configured to store data in a virtual memory space that is segregated from the host memory space (Reuben, 3 Background, Paragraph 8, every guest machines appears to be an independent computer; Fig. 1 each guest OS takes up a portion of the hardware and has to share computer resources with other guest OSes).

9. As per **claim 31**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein malware introduced to the computer system is prevented from moving to another computer system of the networked computer system (Reuben, 4.3 Paragraph 2, the host can view, copy...data stored in the virtual disks…isolation should be provided which avoids the host being a gateway for attacking).

10. As per **claim 32**, Hatfalvi and Reuben disclose the networked computer system of claim 28, wherein the computer system is configured to: communicate with the one or more untrusted network destinations via a first communication connection, communicate with one or more trusted network destinations via a second