

Atty. Docket No.: FORT-012700
Fortinet Ref. No.: 13047

Patent Application

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

MOBILE MALWARE DETECTION AND USER NOTIFICATION

Inventor: **RAINER BAEDER**, residing at:
Schoenblickweg 5
Leinfelden-Echterdingen
70771
GERMANY

Assignee: **FORTINET, INC.**
A Delaware Corporation

Entity: Regular Undiscounted

MOBILE MALWARE DETECTION AND USER NOTIFICATION

COPYRIGHT NOTICE

[0001] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever. Copyright © 2014, Fortinet, Inc.

BACKGROUND

Field

[0002] Embodiments of the present invention generally relate to the field of computer networks. In particular, various embodiments relate to methods and systems for detecting mobile malware and reporting the same to a user concerned with the detected malware.

Description of the related art

[0003] Mobile or portable data processing devices are becoming more common and increasingly powerful. As the processing capabilities of mobile devices, including, but not limited to, mobile phones, smartphones, tablet PCs, and personal digital assistants (PDAs), are increasing, these mobile devices are increasingly becoming targets of computer viruses and other types of malware. Malware typically refers to undesired code, software of a file, which may interrupt the normal functioning of a device and which is usually intended to damage, disable or take partial control over operation of the device or capture personal information. Malicious content may comprise viruses, trojans, worms, or any other malicious programs/code that implement various attacks and may spread across devices.

[0004] At the same time, with the sales of mobile/portable computing devices now exceeding those of laptops and desktops, sensitive and critical data is now frequently transacted on such mobile devices making it more lucrative for intruders or attackers to focus on disrupting the functioning of mobile devices to gain access to them. Furthermore, for several reasons, such as the poor quality and quantum of signature deployment, battery consumption required to run mobile security applications, the software architecture of mobile devices, limitations of mobile device operating systems and complex device management issues, such as potentially limited bandwidth while roaming, among others, security of mobile computing devices is weaker than that of laptops and like devices.

[0005] Existing mobile malware scanners also face issues relating to performing regular updates where malware definition data must be kept up to date in order for them to provide reasonable protection. Malware also changes constantly, requiring continual updates of malware definition at mobile devices to stay current/up to date in order to detect new malware. Furthermore, mobile handsets, especially those with limited processing capability and operating systems or those that do not permit memory access for malware scanning, will require some other method of verifying that resident applications are free of malware. Also, comprehensive signature matching as a virus or malware detection method on memory-constrained devices, like mobile phones, is difficult to efficiently implement due to the need for a large database of identified malware signatures. String matching is also processor intensive and results in a high computational tax on a mobile device, especially when existing mobile platforms have relatively low processing power. Large processing and memory requirements generally result in lower performance and excessive battery drain on mobile devices. Therefore, use of anti-virus or intrusion prevention system (IPS) based security tools installed on the mobile/portable devices are generally not a good fit for current mobile devices.

[0006] There is therefore a need for an improved malware detection and notification system and method for mobile devices.

SUMMARY

[0007] Methods and systems are described for detecting and responding to malware events associated with mobile/portable computing devices by means of a malware detection gateway device associated with a mobile service provider network. According to one embodiment, a malware detection gateway device associated with a mobile service provider network detects a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the mobile service provider network. Responsive thereto, the malware detection gateway device causes a malware reporting/notification message to be sent to a user of the portable computing device by sending a malware indicating message, including an Internet Protocol (IP) address of the portable computing device, to a lookup device.

[0008] Additional aspects of the invention will be set forth in part in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The aspects of the invention will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims. It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0010] FIG. 1 illustrates an exemplary mobile malware detection architecture in accordance with an embodiment of the present disclosure.

[0011] FIG. 2 illustrates exemplary functional modules for detecting and reporting mobile malware in accordance with an embodiment of the present disclosure.

[0012] FIGs. 3A, 3B, and 3C illustrate exemplary embodiments of reporting malware to a user in accordance with various aspects of the present disclosure.

[0013] FIG. 4 is an exemplary sequence block diagram conceptually illustrating malware detection processing in accordance with an embodiment of the present disclosure.

[0014] FIG. 5 illustrates an exemplary representation of a lookup table in accordance with an embodiment of the present disclosure.

[0015] FIG. 6 is an exemplary flow diagram illustrating malware detection and notification processing in accordance with an embodiment of the present disclosure.

[0016] FIG. 7 is an exemplary computer system in which or with which embodiments of the present invention may be utilized.

DETAILED DESCRIPTION

[00017] Methods and systems are described for detecting malware on a mobile/portable computing device by means of a network device, and sending message from the network device to the mobile/portable device upon detection of the malware. Methods and systems are provided for detecting malware on a portable device by a network device that is, for instance, managed by a mobile/network service provider, and notifying the portable device about the potential malware threat. As used herein detecting malware or a malware event generally include, but are not limited to, detection of software, malicious code, macros and the like (e.g., viruses, Trojans, worms, spyware) that may be used to disrupt computer operation, gather sensitive information and/or gain access to private computer systems and detection of an attempt to connect to known or blacklisted Internet Protocol (IP) addresses (e.g., those known to be associated with spam delivery, those known to be compromised, those known to be associated with a botnet, websites having poor reputations or those otherwise known to be associated with fraudulent and/or malicious domains).

[00018] According to one embodiment, method of the present disclosure can include detecting, by means of a malware detection gateway associated with a mobile service provider network, malicious content within a data stream transmitted to/from a portable computing device communicating with a packet data network via the mobile service provider network, and causing a malware reporting/notification message to be sent to a user of the portable computing device, by sending, through the malware detection gateway device, a malware indicating message to a look up device, wherein the malware indicating message comprises an IP address of the portable computing device. In an exemplary implementation, look up device can be configured to receive the malware indicating message from the malware detection gateway device, and then identify/extract user details based on the IP address present in the malware indicating message, based on which the malware reporting/notification message can be sent to the user. According to another exemplary implementation, user details/information extracted from the lookup device can include mobility pattern of the user, calling patterns, message patterns, application usage patterns, types of content being accessed by the portable computing device, among other user attributes.

[00019] According to one embodiment, the malware indicating message can further include one or more of a time of detection of the malware event (e.g., malicious content), a type of malware associated with the malicious content (e.g., adware, backdoor, exploit,

application, flame, monitoring, riskware, rootkit, trojan, work, etc.), a severity of the malware, a security policy violated, a type of security breach, details of the security breach, and properties of the malware.

[00020] According to one embodiment, the malware reporting/notification message can be sent to a user of the portable computing device by the malware detection gateway device based on the response received from the look up device, wherein the response can include user details. According to another embodiment, the malware reporting/notification message can be sent to a user of the portable computing device by the look up device responsive to the malware indicating message. According to another exemplary embodiment, the malware reporting/notification message can be sent to a user of the portable computing device by a network operator of the mobile service provider network responsive to the malware indicating message.

[00021] According to another embodiment, the malware reporting/notification message can be sent to the user through one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, a Multimedia Messaging Service (MMS) message, wherein the malware reporting/notification message can include information regarding the detected malware event and giving the user a set time by which to address the issue (e.g., removal of malicious content).

[00022] According to another embodiment, the malicious content can include one or more of a virus, a trojan, an exploit, an attack, spyware, an expected data stream, blocked content, a security breach and a security violating application. According to another embodiment, the look up device can include or form part of a Policy Control and Resource Function (PCRF) of the mobile service provider network. In yet another embodiment, the look up device can include or form part of a Mobile Device Management (MDM) function of the mobile service provider network.

[00023] According to an embodiment, the malware indicating message can include one or more of a Diameter message a Remote Authentication Dial In User Service (RADIUS) message and a Simple Network Management Protocol (SNMP) message.

[00024] According to another embodiment, malicious content can be detected by performing pattern matching of content of the data stream with one or more of signatures or rules that are defined manually or automatically based on organization policies, or the user/network administrator. In yet another embodiment, malware detection gateway device

can be configured to log the detected malicious content into a log database or any other storage structure.

[00025] According to one embodiment, system of the present disclosure can include a malware detection gateway device logically interposed between a mobile service provider's network and external packet data networks (e.g., an operator-external public packet data network (e.g., the Internet) or operator-external private packet data network or an intra-operator packet data network). In one embodiment, the malware detection gateway device may be physically located within the mobile service provider's network at a reference point between the service provider's packet data network gateway (PDN GW) (e.g., at the Gi interface (for 3G networks), SGi interface (for 4G networks) or the Internet interface or WLAN/Intranet interface (for WLAN networks)) and external packet data networks and maybe may be operatively coupled with a network operator, wherein the malware detection gateway device processes data streams from mobile devices and, using one or more signatures/rules, identifies malicious content transmitted to or from the mobile devices and/or malware running on the mobile devices. The identified malicious content or malware can then be processed to generate a malware-indicating message, which can be sent to a lookup table/device and/or to a mapping database such as Policy Control and Resource Function (PCRF) and/or Mobile Device Management (MDM) for identifying the user(s) impacted by the malware. Identified user(s) can then be notified through a notification means to allow the users to take appropriate action. In the context of the present disclosure, malware is to be broadly construed and may include, but is not limited to, viruses, trojans, exploits, attacks, spyware, expected data stream, blocked content, security breaching data, security violating applications, among other such undesired activities which violoates defined security policies.

[00026] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present invention. It will be apparent to one skilled in the art that embodiments of the present invention may be practiced without some of these specific details.

[00027] Embodiments of the present invention include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, steps may be performed by a combination of hardware, software, firmware and/or by human operators.

[00028] Embodiments of the present invention may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, but is not limited to, fixed (hard) drives, magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs), electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware).

[00029] Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present invention with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present invention may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the invention could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[00030] If the specification states a component or feature “may”, “can”, “could”, or “might” be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[00031] Although the present disclosure has been described with the purpose of detecting and notifying malware to users of portable devices, it should be appreciated that the same has been done merely to illustrate the invention in an exemplary manner and any other purpose or function for which the explained structure or configuration can be used, is covered within the scope of the present disclosure.

[00032] Exemplary embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. These embodiments are provided so that this disclosure will be thorough and complete and will fully convey the scope of the invention to those of ordinary skill in the art. Moreover, all statements herein reciting embodiments of the

invention, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (i.e., any elements developed that perform the same function, regardless of structure).

[00033] Thus, for example, it will be appreciated by those of ordinary skill in the art that the diagrams, schematics, illustrations, and the like represent conceptual views or processes illustrating systems and methods embodying this invention. The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing associated software. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the entity implementing this invention. Those of ordinary skill in the art further understand that the exemplary hardware, software, processes, methods, and/or operating systems described herein are only for illustrative purposes and, thus, are not intended to be limited to any particular construction/structure.

[00034] FIG. 1 illustrates an exemplary mobile malware detection architecture 100 in accordance with an embodiment of the present disclosure. As illustrated, architecture 100 of FIG. 1 can include a wireless packet network 102, which may also interchangeably be referred to as mobile service provider's network 102 hereinafter. Mobile service provider's network 102 may be configured to include one or more communication towers, such as 104 and 106, to provide mobile/wireless access to one or more mobile or portable computing devices. In an example illustration, one or more mobile or portable computing devices, such as device 110-1, device 110-2, device 110-3, device 110-4, and device 110-5, which may collectively and interchangeably be referred to as devices 110 hereinafter, can be configured to access different web services, network resources, and browse various websites from external packet data networks (not shown) using network 102 that is associated with at least one mobile service provider.

[00035] Content/data/information accessed by computing devices 110 from external packet data networks may include malware, such as viruses, attacks, trojans, undesired applications, among other such malware, which may harm the devices 110 or even the functioning of network 102, and/or can put the devices 110 or network 102 at risk as a result of coming into contact with a malicious and/or fraudulent website, for example. According to

one embodiment, architecture 100 therefore includes a logical or physical malware defence platform 112 having one or more malware detection gateway devices, such as 116-1 and 116-2, which may be collectively referred to as malware detection gateway devices 116 hereinafter. According to one embodiment, malware detection gateway devices 116 can be configured, controlled, and/or managed by one or more network operators, such as 114-1 and 114-2, which may be collectively referred to as 114 hereinafter. In another embodiment, platform 112 further includes a lookup device 108 configured to, based on an input attribute, for example, an IP address, identify user details to which the input attribute pertains. Those skilled in the art will appreciate that although platform 112 has been shown separate from network 102, platform 112 or any component therefore of, such as malware detection gateway devices 116 can be configured remotely or locally or may be implemented within network 102, and therefore any such constructions, structures, or architectures are within the scope of the present disclosure.

[00036] According to one embodiment, malware detection gateway device 116 is associated with mobile service provider network 102 and configured to detect malicious content within a data stream transmitted to/from a portable computing device 110 communicating with a packet data network, such as an external network (not shown), via network 102. Malware detection gateway device 116 may also be configured to cause a malware reporting/notification message to be sent to the user of the portable computing device 110 by sending a malware indicating message to lookup device 108, wherein the malware indicating message comprises an IP address of the portable computing device 110. In an exemplary implementation, look up device 108 may be configured to receive the malware indicating message from the malware detection gateway device 116 and then identify/extract user details based on the IP address present in the malware indicating message, based on which the malware reporting/notification message or a similar or different reporting/notification message can be sent to the user of portable computing device 110. According to another exemplary implementation, user details/information extracted by lookup device 108 can include one or more of a mobility pattern of the user, calling patterns, message patterns, application usage patterns, types of content being accessed by portable computing device 110, among other user, device, usage and/or content attributes.

[00037] According to one embodiment, malware detection gateway device 116 is configured to determine details of both the sender (the source) of the malicious content/malware as well as details of the intended recipient of the content based on the

attributes of the content, such as the source-destination IP addresses. Lookup device 108 and/or database or any other repository can be used to extract/map details of the sender and/or of the recipient, wherein the details can include information regarding access/usage history of wireless packet network 102, call logs, messages, among other user, device, usage and/or content details.

[00038] According to one embodiment, the malware indicating message can further include one or more of a time of detection of the malicious content, a type of malware associated with the malicious content, a severity of the malware, a security policy violated, a type of security breach, details of the security breach, and properties of the malware.

[00039] According to one embodiment, the malware reporting/notification message can be sent to the user of portable computing device 110 by malware detection gateway device 116 based on the response received from look up device 108, wherein the response can include user details. The malware reporting/notification message may be sent via an in-band messaging approach (e.g., via a Short Message Service (SMS) message or the like directed to the phone number associated with the device at issue or via an out-of-band messaging approach (e.g., via an SMS message directed to an alternative phone number associated with the user of the device at issue or via an electronic mail (email) message directed to an email account associated with the user of the device at issue). In one embodiment, the malware reporting/notification message can be sent to the user of portable computing device 110 as a result of direction from malware detection gateway device 116. For example, responsive receipt of a command or a malware indicating message from malware detection gateway device 116, look up device 108 may transmit the malware reporting/notification message or the like to the user of portable computing device 110. According to another exemplary embodiment, the malware reporting/notification message can be sent to the user of the portable computing device 110 by a network operator 114 of mobile service provider network 102 responsive to network operator 114 being informed of the malware detection event by way of the malware indicating message or the like.

[00040] According to another embodiment, the malware reporting/notification message can be sent to device 110 through one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, a Multimedia Messaging Service (MMS) message, wherein the malware reporting/notification message can include information regarding the detected malicious content and giving the user a set time by which to address the detected malicious content. When the malware is determined to have been sent from an

external network and directed to device 110, device 110 can be informed of one or more of the name and/or type of malware detected, the source of the malware, the delivery mechanism by which the malware was directed to device 110, potential damage that the malware could have caused, history of the malware, access patterns of device 110, among other information, suggestions, and recommendations.

[00041] According to another embodiment, the malicious content can include one or more of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content, a security breach and a mobile application that violates security policies specified for device 110. According to another embodiment, look up device 108 can include or form part of a Policy Control and Resource Function (PCRF) 118 of mobile service provider network 102/platform 112, wherein PCRF 118 can be configured to return user details based on a unique user identifier provided by malware detection gateway device 116, for example. In yet another embodiment, look up device can include or form part of a Mobile Device Management (MDM) function 120 of mobile service provider network 102/platform 112, wherein MDM functions are typically used to register/deregister mobile devices within mobile network 102. MDM function 120 can be used by an enhanced messaging server, for example, to determine if mobile device 110 is registered (connected) as well as to determine the message delivery path. In an exemplary implementation, lookup device 108 can be configured to determine and return an identity of device 110 with the affected malware in the form of an International Mobile Station Equipment Identity (IMEI) code, an International Mobile Subscriber Identity (IMSI) code, a subscriber number, a mobile number and/or a user identifier of device 110 associated with the supplied input attribute (e.g., an IP address of device 110).

[00042] According to another embodiment, malicious content can be detected by performing pattern matching of content within the data stream with one or more of signatures or rules that are defined manually or automatically based on organization policies, or a user/network administrator. In yet another embodiment, malware detection gateway device 116 can be configured to log the detected malicious content into a log database or any other storage structure. In an example implementation, upon detection of malware on portable device 110, appropriate action(s) can be taken by the user of the portable device 110 and/or by the network operator 114 (if authorized) so as to black list, block, isolate, quarantine or otherwise prevent further access to the detected malware on the device 110 and/or to content attempted to be accessed by the detected malware.

[00043] In another exemplary embodiment, identification of computing device 110 can be done based on the malware indicating message originated by malware detection gateway device 116, which can, in an implementation, include a diameter message or a Remote Authentication Dial In User Server (RADIUS) message that can help the look up device 108 in associating and/or mapping the IP address of user device 110 at any instant of time with an IP assignment/mapping/look up table or database containing IP addresses assigned to user devices 110.

[00044] FIG. 2 illustrates exemplary functional modules 200 for detecting and reporting mobile malware in accordance with an embodiment of the present disclosure. In an aspect, the system described herein for detecting malware on portable computing devices or intended for portable computing devices, such as mobile phones, tablets, smart phones, among others, and for issuing appropriate notifications relating thereto can be implemented by means of one or more processors, a communication interface device, and one or more internal data storage devices operatively coupled to the one or more processors and storing a malware detection module 202, a malware information log generation module 204, a malware-indicating message generation module 206, a user look up module 208, and a malware reporting module 210. One or more of these modules such as malware detection module 202, malware information log generation module 204, malware-indicating message generation module 206, and malware reporting module 210 can be implemented by a first network device associated with a mobile service provider, and one or more of these modules, such as user look up module 208 and malware reporting module 210, can be implemented by a second network device associated with the mobile service provider, wherein the two network devices associated with the network service provider can be logical (virtual) or physical devices. Alternatively, modules 200 may be implemented within a single computing device. Any other number of modules and/or sub-modules can also be incorporated and all such configurations are within the scope of the present disclosure.

[00045] According to one embodiment, malware detection module 202 can be configured to detect malicious content within a data stream transmitted to/from a portable computing device (that forms part of a mobile service provider network) that is communicating with a packet data network. Malware detection module 202 can be configured to detect malicious content, including, but not limited to viruses, trojans, exploits, attacks, spyware, unexpected data streams, blocked content, security breaches, mobile applications that violate one or more security policies and other suspicious user/device

activity identified based on one or more defined parameters/criteria/rules/signatures indicative of the presence of malware.

[00046] In an exemplary implementation, malicious content can be identified by malware detection module 202 by performing pattern matching of content within a data stream received or transmitted by a portable computing device with one or more of signatures or rules or definitions associated with known malicious content. In an exemplary implementation, malware detection module 202 can be configured to maintain a list of signatures, rules and definitions to identify the malicious content, wherein such rules and signatures can be updated in real-time or at periodic intervals. In yet another implementation, signatures/rules/definitions of known malware can be obtained from third party vendors, or can be automatically synchronized with one or more third parties that provide such malware signatures/rules/definitions. In another exemplary implementation, malware detection module 202 can be configured to detect suspicious or unusual activity/behavior by the portable computing device by monitoring data flowing to/from the portable computing device by way of the mobile service provider network.

[00047] According to one embodiment, malware information log generation module 204 can be configured to generate a log of detected malicious content. Malware logs can be used for later offline analysis of detected malware events and/or to facilitate identification of the infected portable computing device(s) or sources of detected malicious content. The log, on one hand, can either be generated for the complete data stream including the malware, or can be generated only for the malicious content. Any other possible combination or format can also be used to create and update the log in real time. In an embodiment, for each detected malware, a log entry may be created with multiple fields including, but not limited to, the IP address of the mobile device for which the malware was detected, destination information, type of malware, severity of malware, details of malware, security policy violated by the malware, time of detection, among other parameters. Collected logs can also be used to update the signatures and/or rules that can later be used by malware detection module 202.

[00048] According to one embodiment, the malware-indicating message generation module 206 is configured to enable malware detection gateway device 116 to generate a malware indicating message based on various parameters associated with the malware detected by malware detection module 202, and to send the generated malware indicating message to a lookup device for determination of user details pertaining to the detected malware. According to embodiment, the malware indicating message can include an IP

address of the portable computing device to which the detected malware was intended, from which the detected malware was originated and/or on which the detected malware was found to reside. According to another embodiment, the malware-indicating message may include several details relating to the detected malware, including, but not limiting to, the IP address of the infected/targeted portable computing device or the IP address of the external source of the malware, a timestamp indicating a time and/or date of the malware detection, information regarding a security policy violated, the type of malware detected, information regarding the severity of the detected malware, information or a link to information regarding how to remediate or protect the infected portable computing device or otherwise remove or disable the detected malware, information or a link to information providing a description of the detected malware. Malware-indicating message generation module 206 can be configured to send the generated malware-indicating message through a suitable communication means to the lookup device that can be configured to implement the look up module 208. In an example implementation, the malware indicating message generation module 206 can be configured to send malware-indicating message to the look up module 208 using a wired/wireless data network if the two modules are configured to be implemented on different computing devices, or can be configured to send the malware-indicating message to look up module 208 using a data bus if the two modules are configured to be implemented on the same computing device. According to one embodiment, the malware-indicating message can include a diameter message or Remote Authentication Dial In User Server (RADIUS) message that can help the look up module 208 to identify the portable device/user. In an exemplary implementation, the Diameter and/or RADIUS message can include information such as “IP address 192.168.123.XXXX; timestamp 123432345; violated security policy MN; malware code 1232; severity BBBB; source information; frequency;”, among other like parameters.

[00049] According to one embodiment, user lookup module 208 can be configured to receive the malware indicating message from the malware indicating message generation module 206, and identify a user/portable computing device corresponding to the IP address received as part of the malware-indicating message along with the time of malware detection. In an exemplary implementation, user lookup module 208 can be configured to identify the user/portable computing device corresponding to the IP address received as part of the malware-indicating message using a look up table that includes a mapping of the IP address with the user identifiers such as International Mobile Station Equipment Identity (IMEI) code and International Mobile Subscriber Identity (IMSI) code. In an exemplary implementation,

the mapping table can keep an updated record of IP addresses assigned to different portable computing devices/users (at various times) along with their identifiers, which can be used by the user lookup module 208 to identify the user was assigned the IP address at issue at during the timeframe at issue (e.g., at the time of the malware detection). Based on the IP address of the device associated with the detected malware and the time of malware detection, user lookup module 208 can determine the identity of the user/portable computing device using the mapping table. According to one embodiment, apart from user identity, attributes of the user such as browsing history, call logs, message logs, usage pattern, among others can also be retrieved and processed to arrive at meaningful information that may assist the user or the mobile service provider in connection with countering the malware.

[00050] In an aspect, the look up device can include or form part of a Policy Control and Resource Function (PCRF) of the mobile service provider network. In another aspect, the look up device can include or form part of a Mobile Device Management (MDM) function of the mobile service provider network.

[00051] Upon detection of malware and the identification of user/portable computing device, malware reporting module 210 may be configured to send an alert message along with one or more recommendations and/or suggested action items to the affected user/portable computing device. According to one embodiment, malware reporting module 210 can be configured to notify the identified user of the malicious content being generated and/or being processed by him/her. In an implementation, the user can be sent a notification that is indicative of the nature of malware, extent of security policy breach, severity of malware, potential impact and/or consequences of the malware, along with suggestions that need to be complied with. The user can also be given a stipulated amount of time to implement the suggested solution, or take action(s) to rectify the identified problem. In an exemplary implementation, the malware-reporting module 210 can be configured to, automatically generate and send the malware reporting/notification message to the user based on and responsive to receipt of the malware indicating message from lookup device 108.

[00052] In an exemplary implementation, the malware reporting/notification message can include malware alerts with other specific details including, but not limiting to, type of malware associated with the malicious content, severity of the malware, security policy violated, type of security breach, details of the security breach, properties of the detected malware and one or more alternate appropriate actions that can be taken by the user/portable computing device for neutralizing the malware. In another exemplary implementation, the

malware reporting/notification message can include details about applications/websites/services that may be associated with the malicious content and rectification measure that should be taken to prevent future infection. According to one embodiment of the present disclosure, malware reporting module 210 can be configured to send a malware reporting/notification message to the portable device/user in the form of a Short Message Service (SMS) message, an automated telephone call, an electronic mail (email) message or a Multimedia Messaging Service (MMS) message.

[00053] According to one embodiment, a first network device, also interchangeably referred to as a malware detection gateway device, can be configured to include malware detection module 202, malware information log generation module 204, malware-indicating message generation module 206, malware reporting module 210; and a second network device, also interchangeably referred to as a look up device, can be configured to include user look up module 208 and malware reporting module 210. In an exemplary implementation, the malware detection gateway device and the look up device can be configured to be logically or physically present on the same computing device or on different computing devices. One or more of these modules can also be implemented by a third party/a third network device, wherein, for instance, the malware reporting module 210 can be configured to be implemented by a third party that is configured to provide malware reporting and removal.

[00054] In an exemplary implementation, malware reporting/notification message generated by the malware reporting module 210 can be sent to the identified portable computing device/user by the malware detection gateway device responsive to receiving user details from the look up device, or directly by the look up device responsive to the malware indicating message, or by any other network device associated with network server provide responsive to receiving the malware indicating message and identified user details.

[00055] FIGs. 3A, 3B, and 3C illustrate various malware detection and reporting scenarios in accordance with embodiments of the present disclosure. As illustrated in FIG. 3A, malware detection gateway device 302 may be configured to detect malware based on rules/signatures/patterns/conditions, generate a malware indicating message, including an IP address associated with the affected mobile device and attributes/parameters of the detected malware, receive user details from PCRF/MDM/look up device 304 based on the malware indicating message, and finally send a malware reporting/notification message to a user 306 of the affected mobile device based on the received user details.

[00056] In another embodiment, as illustrated in FIG. 3B, malware detection gateway device 312 can be configured to detect malware, generate and send a malware indicating message to a PCRF/MDM/look up device 314, and enable the look up device 314 to process the received malware indicating message to generate intended user details and further enable the lookup device 314 to directly send the malware reporting/notification message to the intended user based on the generated user details.

[00057] In yet another embodiment as illustrated in FIG. 3C, malware detection gateway device 322 can be configured to detect the malware and generate/send a malware indicating message to a PCRF/MDM/look up device 324 based on the detected malware. The lookup device 324 can then, process the malware indicating message to identify user details corresponding to the attributes present in the malware indicating message, and send the user details to a network operator 326, who can then send the malware reporting/notification message to the identified user 328.

[00058] FIG. 4 illustrates an exemplary block diagram 400 illustrating malware detection processing in accordance with an embodiment of the present disclosure. As illustrated in FIG. 4, an exemplary implementation of the proposed system of the present disclosure includes detection of malware in incoming/outgoing data stream (bit pattern, data packets, visited websites, downloaded content, applications, and among other type of content) being accessed by one or more portable computing devices as shown in block 402. The detection can either be performed at a malware detection gateway device or at any other appropriate network device within a mobile service provider's network that is configured to receive data packets and based on one or more filters/criteria/rules, identify potential malicious content in transit or activity indicative of the existence of malware resident on a subscriber's mobile device.

[00059] At block 404, malware detection gateway device 116 generates and/or updates one or more malware logs based on the detected malware. At block 406, malware detection gateway device 116 generates a malware-indicating message based on the detection event, wherein the malware-indicating message can include information/attributes of malware along with user identifier information, such as an IP address of the mobile device at issue. Such a malware-indicating message can be sent to a lookup/mapping table 408 so as to extract user details corresponding to the user identifier information. As shown, lookup/mapping table 408 can be configured to store a mapping of IP addresses to User details, such as username, phone number, IMEI number, user attributes, history, phone logs, message logs, browsing history,

among any other desired information. Those skilled in the art will appreciate that table 408 is a non-limiting conceptual illustration of a potential mapping and that such a mapping can be implemented in various manners. For example, the lookup process may involve a database query of a database associated with the mobile service provider's network.

[00060] As shown in FIG. 4, based on the user details retrieved from the lookup table 408, a network operator 410 can then issue a notification/reporting message to the user 412 associated with the affected mobile device in order to inform user 412 to take necessary actions, such as installing anti-virus software, avoiding particular web sites, etc. Network operator 410 may also take certain actions, such as blocking the user, reporting the activity to the organization, or any other action that can be envisaged. Network operator 410 may serve a quality control function for automatically generated notification/reporting messages, may manually generate all or some portions of the notification/reporting messages and/or may inform customer service representatives to contact user 412.

[00061] FIG. 5 illustrates an exemplary conceptual representation 500 of a lookup table in accordance with an embodiment of the present disclosure. Allocation of IP addresses by a network service provider (e.g., a mobile service provider) to user/portable computing devices may be dynamic in nature, and hence dynamic updates to look-up table 500 may be required. In a wireless network system, dynamic IP addresses can be assigned to a portable computing device when it needs to connect to a data network, for example.

[00062] In an example implementation, look table 500, as shown in FIG. 5, can be used by a PCRF/MDM/look up device to identify a user and/or associated user details that are associated with the IP address associated with the detected malware event. According to one embodiment, look up table 500 can be used for mapping of the IP address, received as part of the malware indicating message, with user identifiers/identification information, such as an IMEI code and/or an IMSI code, in order to identify the user and/or the specific portable computing device corresponding to the affected IP address. In an example implementation, look up table 500 can keep an updated record of IP addresses assigned to different portable computing devices/users along with their identifiers/details for multiple predefined or configurable timeframes. Based on the IP address of the mobile device associated with the malware detection event and time of malware detection, lookup table 500 can be used to determine the identity of the user/portable computing device. In the context of the present example, if the IP address specified within a malware indicating message received by lookup table 500 was 172.116.254.1 and the time of malware detection is specified as 5 PM, then

user 4 is the affected user to which the malware reporting/notification message will be directed. Those skilled in the art will appreciate lookup table 500 changes over time as the mobile service provider dynamically assigns IP addresses to mobile devices of its subscribers and that such dynamic assignment results in the same IP address being associated with different users at different points in time. In an exemplary implementation, a network/mobile service provider can use a set of dynamic IP addresses, and can assign these IP addresses to different users at different points of time. For example, when a new user moves from one tower to another, the user's portable computing device may release its current IP address and be assigned a new one by the network/service provider. As can be seen from the FIG. 5, the same IP address (e.g., 172.116.254.1) may have been associated with several different users at differing times over the course of a span of hours. In the context of the present example, IP address 172.116.254.1 was associated with user 3 at 3 PM, with user 4 at 5 PM, with user 2 at 7 PM and with user 1 at 9 PM. Therefore it should be clear that the same IP address can be assigned to different users at different times and a single user can be assigned different IP address at different time. It is also possible to assign a static IP address to a given portable computing device, which greatly simplifies this lookup process. Any such dynamic or static assignment of IP addresses to mobile devices of a mobile service provider is within the scope of the present disclosure.

[00063] Though lookup table 500 illustrates mapping of IP addresses to usernames, it is within the scope of present disclosure to map IP addresses to various other identifiers, such as IMEI codes, IMSI codes or mobile telephone numbers.

[00064] FIG. 6 is an exemplary flow diagram 600 illustrating malware detection and notification processing in accordance with an embodiment of the present disclosure. Example implementations described herein are directed to methods of detecting (i) malicious content in transit through a mobile service provider network that originated from a mobile device of a subscriber or is directed to a mobile device of a subscriber; or (ii) other activity indicative of the existence of malware on a mobile device of a subscriber; and responsive thereto automatically generating and sending a malware notification message to the affected user.

[00065] At step 610, a malware detection gateway device that is associated with a mobile service provider network can detect a malware event, e.g., malicious content within a data stream transmitted to/from a portable computing device communicating with a packet

data network via the mobile service provider network or activity indicative of the existence of malware resident on the portable computing device.

[00066] At step 620, the malware detection gateway device can process the detected malware to generate a malware indicating message that, apart from malware attributes/parameters, includes an IP address of the portable computing device, and send the generated message to a lookup device.

[00067] At step 630, the lookup device can map the IP address received as part of the malware indicating message to user details of the portable computing device. Finally, at step 640, the retrieved user details can be used to send a malware reporting/notification message to the user of the portable computing device. The malware reporting/notification message may inform the user of one or more actions to take to prevent and/or remediate the situation. The malware reporting/notification message may also specify a timeframe within which the user must perform the actions. In one embodiment, upon expiration of the specified timeframe, the mobile service provider may take affirmative action to protect its network and/or other subscribers against harm from the mobile device in question by deactivating the user's service, for example.

[00068] FIG. 7 is an example of a computer system 700 with which embodiments of the present disclosure may be utilized. Computer system 700 may represent or form a part of a one or more logical or physical network devices (e.g., malware detection gateway device 115, lookup device 108) operable within or otherwise associated with a mobile service provider network.

[00069] Embodiments of the present disclosure include various steps, which have been described above. A variety of these steps may be performed by hardware components or may be tangibly embodied on a computer-readable storage medium in the form of machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with instructions to perform these steps. Alternatively, the steps may be performed by a combination of hardware, software, and/or firmware.

[00070] As shown, computer system 700 includes a bus 730, a processor 705, communication port 710, a main memory 715, a removable storage media 740, a read only memory 720 and a mass storage 725. A person skilled in the art will appreciate that computer system 700 may include more than one processor and communication ports.

[00071] Examples of processor 705 include, but are not limited to, an Intel® Xeon® or Itanium® processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines

of processors, FortiSOC™ system on a chip processors or other future processors. Processor 705 may execute instructions associated with one or more of the various functional modules associated with malware defence platform 112. As such, processor may represent and/or perform the functionality of one or more of malware detection module 202, malware information log generation module 204, malware-indicating message generation module 206, user lookup module 208 and/or malware reporting module 210.

[00072] Communication port 710 can be any of an RS-232 port for use with a modem based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. Communication port 710 may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), or any network to which computer system 700 connects.

[00073] Memory 715 can be Random Access Memory (RAM), or any other dynamic storage device commonly known in the art. Read only memory 720 can be any static storage device(s) such as, but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information such as start-up or BIOS instructions for processor 705.

[00074] Mass storage 725 may be any current or future mass storage solution, which can be used to store information and/or instructions. Exemplary mass storage solutions include, but are not limited to, Parallel Advanced Technology Attachment (PATA) or Serial Advanced Technology Attachment (SATA) hard disk drives or solid-state drives (internal or external, e.g., having Universal Serial Bus (USB) and/or Firewire interfaces), such as those available from Seagate (e.g., the Seagate Barracuda 7200 family) or Hitachi (e.g., the Hitachi Deskstar 7K1000), one or more optical discs, Redundant Array of Independent Disks (RAID) storage, such as an array of disks (e.g., SATA arrays), available from various vendors including Dot Hill Systems Corp., LaCie, Nexsan Technologies, Inc. and Enhance Technology, Inc.

[00075] Bus 730 communicatively couples processor(s) 705 with the other memory, storage and communication blocks. Bus 730 can be, such as a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus, Small Computer System Interface (SCSI), USB or the like, for connecting expansion cards, drives and other subsystems as well as other buses, such a front side bus (FSB), which connects processor 705 to system memory.

[00076] Optionally, operator and administrative interfaces, such as a display, keyboard, and a cursor control device, may also be coupled to bus 730 to support direct operator

interaction with computer system 700. Other operator and administrative interfaces can be provided through network connections connected through communication port 710.

[00077] Removable storage media 740 can be any kind of external hard-drives, floppy drives, IOMEGA® Zip Drives, Compact Disc – Read Only Memory (CD-ROM), Compact Disc – Re-Writable (CD-RW), Digital Video Disk – Read Only Memory (DVD-ROM).

[00078] Components described above are meant only to exemplify various possibilities. In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

[00079] While embodiments of the present invention have been illustrated and described, it will be clear that the invention is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the invention, as described in the claim.

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	FORT-012700
		Application Number	
Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		
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 fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove				
Legal Name				
Prefix	Given Name	Middle Name	Family Name	Suffix
	Rainer		Baeder	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Leinfelden-Echterdingen		Country of Residence i	DE
Mailing Address of Inventor:				
Address 1		Schoenblickweg 5		
Address 2				
City	Leinfelden-Echterdingen		State/Province	
Postal Code	70771		Country i	DE
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	64128
Email Address	Add Email Remove Email

Application Information:

Title of the Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		
Attorney Docket Number	FORT-012700	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	1

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-012700
		Application Number	
Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		

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.

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	64128		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the application number blank.

Prior Application Status		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button. Add			

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-012700
		Application Number	
Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		

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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(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 ^j (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

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.
--

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-012700
		Application Number	
Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		

If 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 World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

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		Remove
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 Fortinet, Inc.

Mailing Address Information:

Address 1	1090 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country ⁱ	US	Postal Code	94086
Phone Number		Fax Number	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-012700
		Application Number	
Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			Add

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.			
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.			
			Remove
If the Assignee or Non-Applicant Assignee is an Organization check here.			☒
Organization Name	Fortinet, Inc.		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	1090 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country i	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			Add

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Michael A DeSanctis/		Date (YYYY-MM-DD)	2015-02-09	
First Name	Michael A.	Last Name	DeSanctis	Registration Number	39957
Additional Signature may be generated within this form by selecting the Add button.				Add	

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	FORT-012700
		Application Number	
Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION		

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

Privacy Act Statement

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

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

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

100

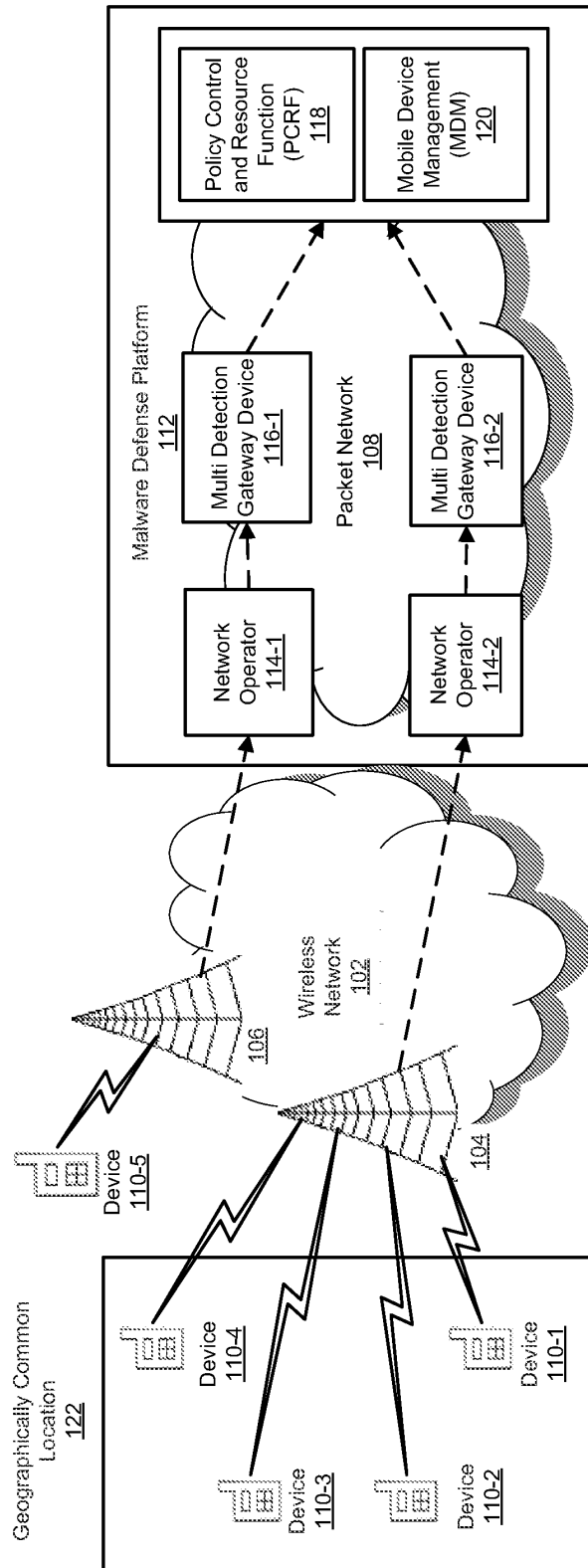


FIG. 1

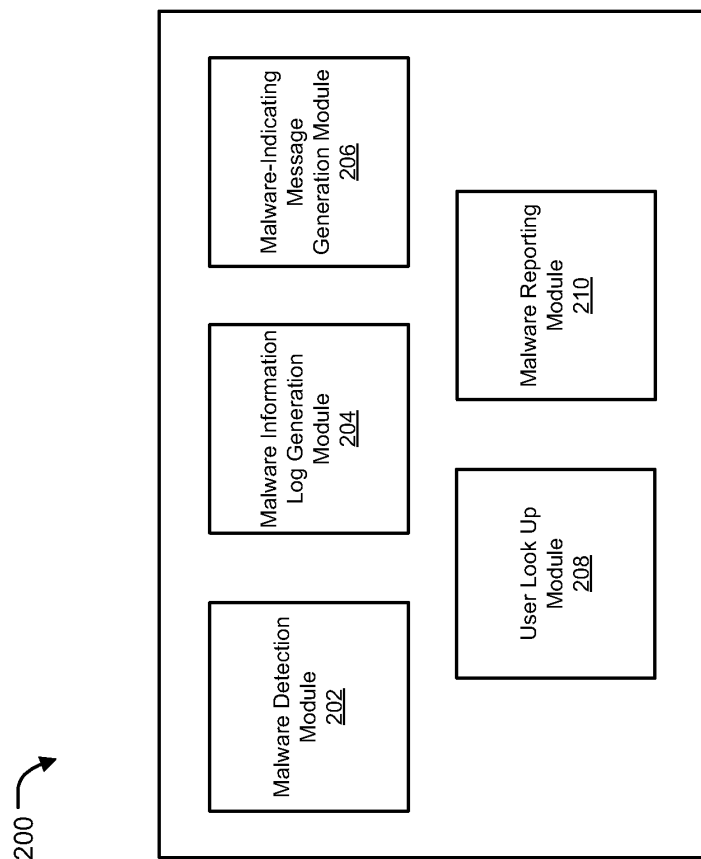


FIG. 2

300 ↗

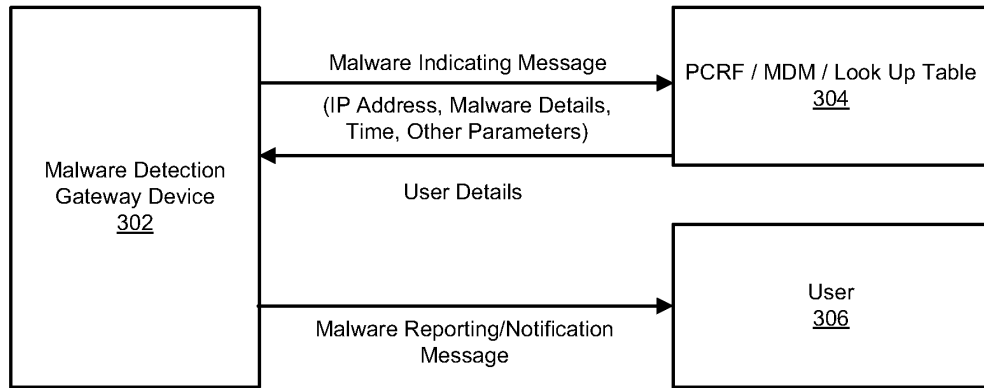


FIG. 3A

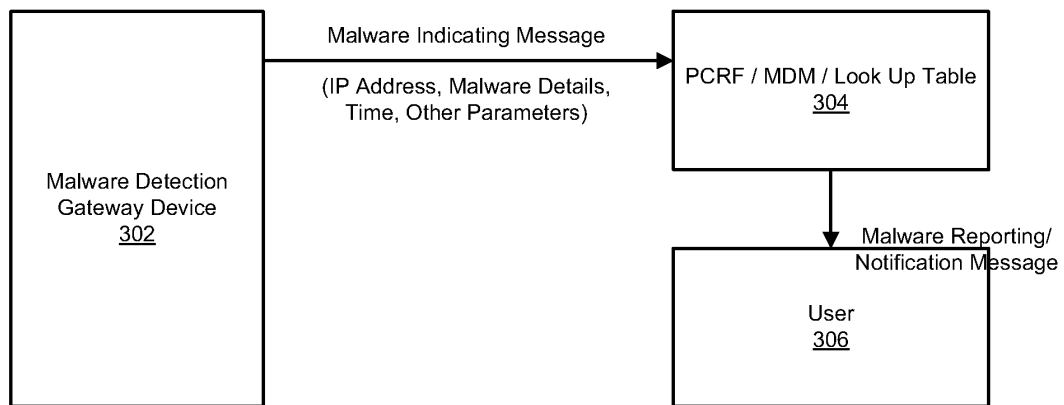


FIG. 3B

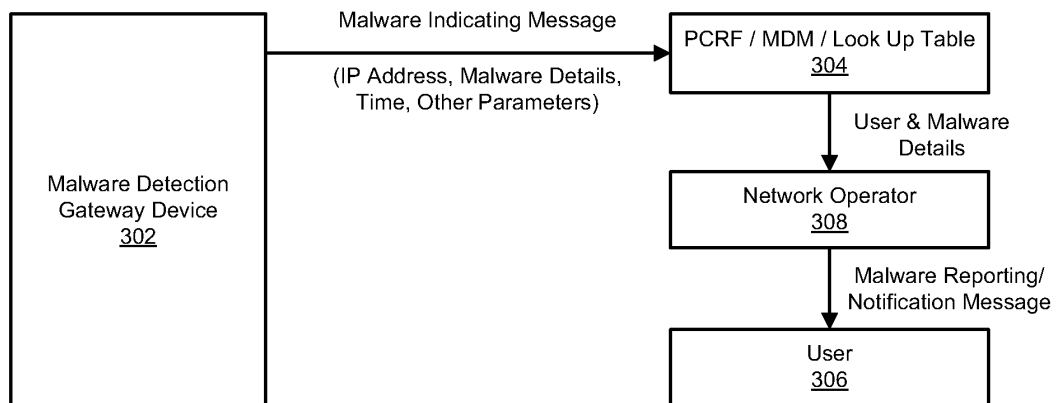


FIG. 3C

+

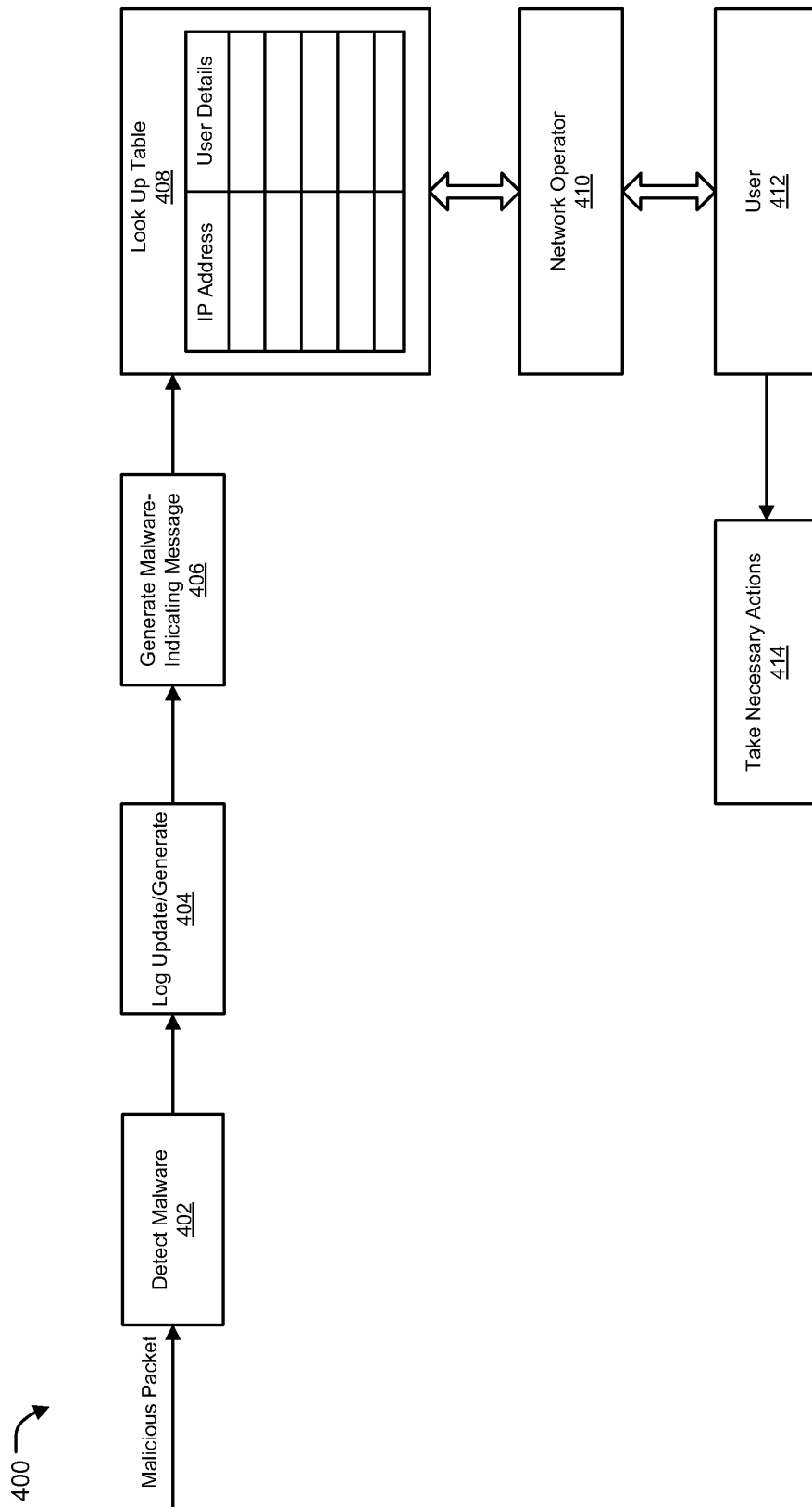


FIG. 4

+

500 

IP address / Time	3 PM	5 PM	7 PM	9 PM
172.116.254.1	User 3	User 4	User 2	User 1
192.168.100.1	User 4	User 3	User 3	User 4
172.163.123.1	User 2	User 1	User 4	User 2
192.166.165.1	User 1	User 2	User 1	User 3

FIG. 5

+

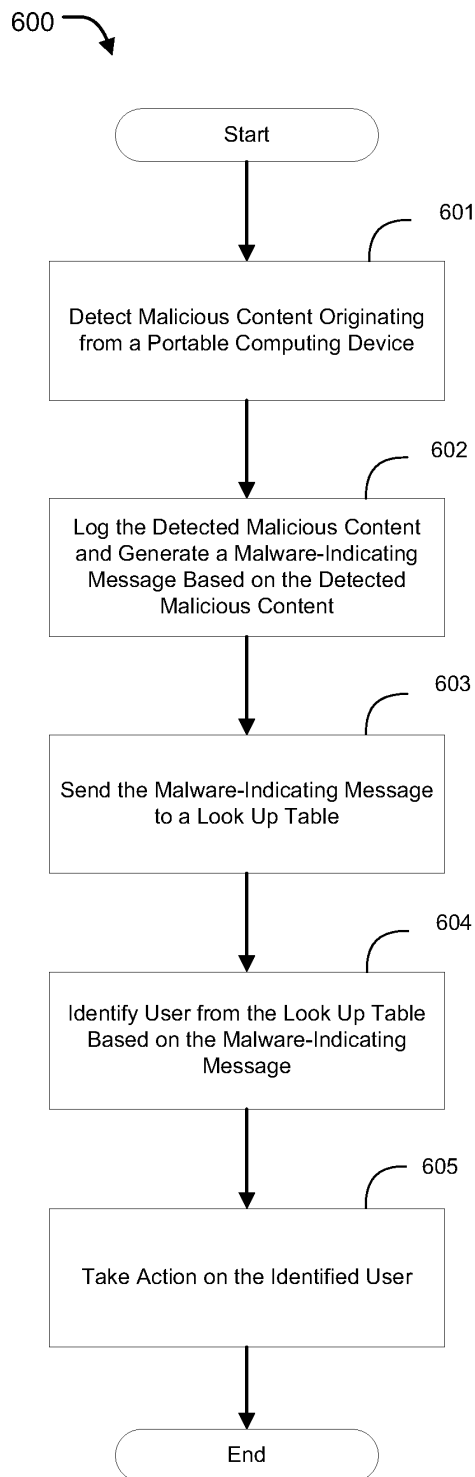


FIG. 6

700 →

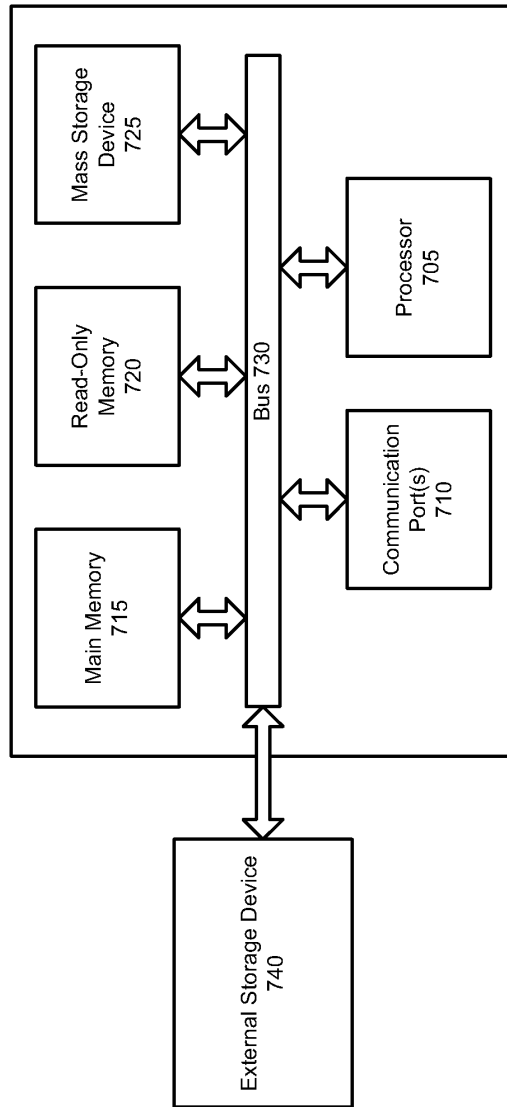


FIG. 7

CLAIMS

What is claimed is:

1. A method comprising:
 - detecting, by a malware detection gateway device associated with a mobile service provider network, a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the mobile service provider network; and
 - causing a malware reporting/notification message to be sent to a user of the portable computing device, by sending, by the malware detection gateway device, a malware indicating message to a lookup device, wherein the malware indicating message comprises an Internet Protocol (IP) address of the portable computing device.
2. The method of claim 1, wherein said detecting a malware event comprises observing activity of the portable computing device that is indicative of malware resident on the portable computing device.
3. The method of claim 1, wherein said detecting a malware event comprises detecting malicious content within the data stream.
4. The method of claim 3, wherein said detecting malicious content comprises performing pattern matching of content within the data stream with one or more of signatures or rules.
5. The method of claim 1, wherein the malware event is associated with one or more of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content, a security breach and a security violating application.
6. The method of claim 1, wherein the malware indicating message further comprises one or more of a time of detection of the malicious content, a type of malware associated with the malware event, a severity of the malware, a security policy

violated, a type of security breach, details of the security breach, and properties of the malware.

7. The method of claim 1, wherein said causing a malware reporting/notification message to be sent to a user of the portable computing device comprises sending, by the malware detection gateway device, the malware reporting/notification message to the user responsive to receiving user details from the lookup device.
8. The method of claim 1, wherein said causing a malware reporting/notification message to be sent to a user of the portable computing device comprises triggering the malware reporting/notification message to be sent by the lookup device responsive to the malware indicating message.
9. The method of claim 1, wherein said causing a malware reporting/notification message to be sent to a user of the portable computing device comprises triggering the the malware reporting/notification message to be sent by a network operator of the mobile service provider network responsive to the malware indicating message.
10. The method of claim 1, wherein the malware reporting/notification message comprises one or more of sending the user one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, a Multimedia Messaging Service (MMS) message and wherein the malware reporting/notification message includes information regarding the malware event and giving the user a set time by which to address the malware event.
11. The method of claim 1, wherein the lookup device includes or forms part of a Policy Control and Resource Function (PCRF) of the mobile service provider network.
12. The method of claim 1, wherein the lookup device includes or forms part of a Mobile Device Management (MDM) function of the mobile service provider network.
13. The method of claim 1, wherein the malware indicating message comprises a Diameter message.

14. The method of claim 1, wherein the malware indicating message comprises a Remote Authentication Dial In User Service (RADIUS) message.
15. The method of claim 1, further comprising, responsive to receipt of the malware indicating message, identifying the user by the lookup device based on the IP address.
16. The method of claim 14, further comprising extracting information relating to the user, wherein the information comprises calling patterns, message patterns, application usage patterns, types of content accessed by the portable computing device and user attributes.
17. The method of claim 1, further comprising logging, by the malware detection gateway, information regarding the malware event.
18. A malware detection system operable within a mobile service provider network comprising:
 - one or more processors;
 - a communication interface device;
 - one or more internal data storage devices operatively coupled to the one or more processors and storing instructions representing:
 - a malware detection module configured to detect malicious content within a data stream originating from or directed to a portable computing device communicating with a packet data network via the mobile service provider network;
 - a user lookup module configured to identify a user corresponding to the portable computing device based on a lookup table and a unique identifier associated with the portable computing device; and
 - a malware-indicating message module configured to query the user lookup module by providing information relating to the detected malicious content and the unique identifier;
 - a malware reporting module configured to notify the user of the detected malicious content.

19. The system of claim 18, wherein the information relating to the detected malicious content comprises one or a combination of a time of detection, a type of malware, severity of the malware, a security policy violated, a type of security breach, details of the security breach and properties of the malware.
20. The system of claim 18, wherein the unique identifier comprises an Internet Protocol (IP) address associated with the portable computing device.
21. The system of claim 18, wherein the malware reporting module is further configured to send a notification to the user in a form of one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, a Multimedia Messaging Service (MMS) message and wherein the notification includes information regarding the detected malicious content and giving the user a set time by which to take action to address the detected malicious content.
22. The system of claim 18, wherein malicious content comprises one or a combination of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content and a security breach or a security violation.
23. The system of claim 18, wherein the lookup table forms part of a Policy Control and Resource Function (PCRF) of the mobile service provider network.
24. The system of claim 18, wherein the lookup table forms part of a Mobile Device Management (MDM) function of the mobile service provider network.
25. The system of claim 18, wherein the lookup table is stored in a database operatively coupled with the mobile service provider network.
26. The system of claim 18, wherein the malware-indicating message module queries the user lookup module by sending the user lookup module a Diameter message.
27. The system of claim 18, wherein wherein the malware-indicating message module queries the user lookup module by sending the user lookup module a Remote Authentication Dial In User Service (RADIUS) message.

28. The system of claim 18, wherein the user lookup module is further configured to extract information relating to the user, wherein the information comprises calling patterns, message patterns, application usage patterns, types of content accessed by the portable computing device and user attributes.
29. The system of claim 18, wherein the malware detection module is further configured to apply one or more rules to content within the data stream or match the content with one or more signatures.
30. The system of claim 18, further comprising a malware information log generation module configured to log information regarding detected malicious content.
31. The system of claim 18, wherein the portable computing device comprises a smartphone, a mobile phones a Personal Digital Assistant (PDA) or a tablet personal computer.

Electronic Acknowledgement Receipt	
EFS ID:	21445089
Application Number:	14617787
International Application Number:	
Confirmation Number:	1008
Title of Invention:	MOBILE MALWARE DETECTION AND USER NOTIFICATION
First Named Inventor/Applicant Name:	Rainer Baeder
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012700
Receipt Date:	09-FEB-2015
Filing Date:	
Time Stamp:	19:36:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 2480
RAM confirmation Number	6091
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	ads.pdf	1560934	no	7
			050432f675e02ac0e64894c8e778ff86254ed30		
Warnings:					
Information:					
2	Oath or Declaration filed	Declaration.pdf	1679485	no	1
			b5b5c610e448654a5cee5b6032464659aff123a		
Warnings:					
Information:					
3	Drawings-only black and white line drawings	drawings.pdf	41810	no	7
			de6df73e18bdbb41427b91a98e1052305743a655		
Warnings:					
Information:					
4	Assignee showing of ownership per 37 CFR 3.73.	statement.pdf	117087	no	3
			4a3a306383bd8237363b110b4d20a64fadd45c93		
Warnings:					
Information:					
5	Assignee showing of ownership per 37 CFR 3.73.	Assignment.pdf	2744150	no	2
			69f37962167313de82fdb84dc747707fd9016e4b		
Warnings:					
Information:					
6	Power of Attorney	Executed_POA_3_73_c_2.pdf	76400	no	1
			f4ad760f71d7becdc33b00b6c2c4b21776d380d1		
Warnings:					
Information:					
7		Patent_Application.pdf	247236	yes	30
			cdc0f0a7f7aa3f28f56b35da6d0ca00c743272ee		
	Multipart Description/PDF files in .zip description				
	Document Description	Start	End		

	Specification		1		24
	Claims		25		29
	Abstract		30		30
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	36594	no	2
			a81aaacb7d1d624b826f6444870efd42e3c7ffdb		
Warnings:					
Information:					
Total Files Size (in bytes):			6503696		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Fortinet, Inc.

Application No./Patent No.: _____ Filed/Issue Date: February 9, 2015

Titled: MOBILE MALWARE DETECTION AND USER NOTIFICATION

Fortinet, Inc., a corporation

(Name of Assignee)

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

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

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is _____. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

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

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

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

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

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

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

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

2. From: _____ To: _____

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

[Page 1 of 2]

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

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

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

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

4. From: _____ To: _____

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

5. From: _____ To: _____

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

6. From: _____ To: _____

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

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

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

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

/Michael A DeSanctis/

Signature

Michael A. DeSanctis

Printed or Typed Name

February 9, 2015

Date

39957

Title or Registration Number

[Page 2 of 2]

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		MOBILE MALWARE DETECTION AND USER NOTIFICATION		
First Named Inventor/Applicant Name:		Rainer Baeder		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-012700		
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	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Pages:				
Claims:				
Claims in Excess of 20	1202	11	80	880
Miscellaneous-Filing:				
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 (\$)				2480

ASSIGNMENT

WHEREAS, I, Rainer Baeder, have invented certain new and useful improvements for which an application entitled

"MOBILE MALWARE DETECTION AND USER NOTIFICATION"

is about to be made for Letters Patent of the United States, the application having been executed on even date herewith, and which may be identified in the United States Patent and Trademark Office by Application No. _____, filed on _____ and further identified as Atty. Docket No. FORT-012700.

WHEREAS, Fortinet, Inc., a Corporation of the State of Delaware, and having its principal offices at 1090 Kifer Rd., Sunnyvale, CA 94086 (hereafter "Assignee"), is desirous of acquiring the entire right, title and interest in and to the application, any inventions or discoveries described therein and in, to and under any and all Letters Patents to be obtained therefor;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I have sold, assigned and transferred, and by these presents do hereby sell, assign and transfer unto the Assignee, its successors and assigns:

1. the entire right, title and interest in and to the application, any inventions or discoveries described therein and the Letters Patent(s), both foreign and domestic, that may or shall issue, including all rights under the International Convention, and
2. all proceeds of the application, any inventions or discoveries described therein and the Letters Patent(s) (including but not limited to, damages for pre-patent grant infringement, all license royalties and proceeds of infringement suits); and in and to any and all causes of action (excepting claims upon the United States of America) for past, present, and future infringement of any of the Letters Patent(s), or relating to any inventions or discoveries described therein, including the right to collect royalties and seek injunctive relief, for all such infringements and the right to sue on all such causes of action for their own use and benefit and the use and benefit of their successors, assigns and legal representatives,

I do hereby authorize and request the Commissioner of Patents to issue the Letters Patent(s) to the Assignee in accordance herewith.

I hereby authorize the Assignee, its successors and assigns or anyone it may properly designate, to insert in this instrument the filing date and Application No. of the application when ascertained.

I further authorize the Assignee, its successors and assigns, or anyone it may properly designate, to apply for Letters Patent, in its own name, if desired, in any and all foreign countries, and additionally to claim the filing date of the United States application and/or otherwise take advantage of the provisions of the International Convention.

I do hereby covenant and agree with the Assignee, its successors and assigns, that I will not execute any writing or do any act whatsoever conflicting with these presents, and that I or my executor(s) or administrator(s) will, at any time upon request, without further or additional consideration, but at the expense of the Assignee, its successors and assigns, execute such additional writings and do such additional acts as the Assignee, its successors and assigns, may deem necessary or desirable to perfect the Assignee's enjoyment of this grant, and render all necessary assistance in making application for and obtaining original, continuation, divisional, reissued, reexamined, substitute or extended Letters Patent(s) of the United States, or of any and all foreign countries on the invention, and in enforcing any rights, occurring as a result of such applications or patents, by giving testimony in any proceedings or transactions involving such applications or patents.

IN WITNESS WHEREOF, I have executed this Assignment on the date indicated below.

Signature:	<i>Rainer Baedler</i>
Date:	2017/02/09
Full Name:	Rainer Baedler
Address:	Schoenblickweg 5
	Leinfelden-Echterdingen 70771
	GERMANY

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 TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:



Practitioners associated with Customer Number:

64128

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:



The address associated with Customer Number:

64128

OR

☐	Firm or Individual Name			
	Address			
	City	State	Zip	
	Country			
	Telephone	Email		

Assignee Name and Address: Fortinet, Inc.
899 Kifer Rd.
Sunnyvale, CA 94086

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date
Name	Todd A. Nelson	Telephone (408) 486-7803
Title	Vice President Legal	

This collection of information is required by 37 CFR 1.31, 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.

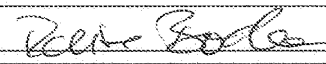
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ABSTRACT

[00080] Methods and systems for detecting and responding to malware events associated with mobile/portable computing devices by means of a malware detection gateway device associated with a mobile service provider network are provided. According to one embodiment, a malware detection gateway device associated with a mobile service provider network detects a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the mobile service provider network. Responsive thereto, the malware detection gateway device causes a malware reporting/notification message to be sent to a user of the portable computing device by sending a malware indicating message, including an Internet Protocol (IP) address of the portable computing device, to a lookup device.

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.

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

Title of Invention	MOBILE MALWARE DETECTION AND USER NOTIFICATION
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 _____ filed on _____ 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 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:	Rainer Baeder
Date (Optional):	20/02/09
Signature:	
Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form 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. 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.

SCORE Placeholder Sheet for IFW Content

Application Number: 14617787

Document Date: 02/09/2015

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://Score.uspto.gov/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013



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
14/617,787	02/09/2015	2431	2480	FORT-012700	31	2

CONFIRMATION NO. 1008

FILING RECEIPT



64128
MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

Date Mailed: 02/25/2015

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)

Rainer Baeder, Leinfelden-Echterdingen, GERMANY;

Applicant(s)

Fortinet, Inc., Sunnyvale, CA

Assignment For Published Patent Application

FORTINET, INC., Sunnyvale, CA

Power of Attorney: The patent practitioners associated with Customer Number 64128

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 02/24/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/617,787**

Projected Publication Date: 08/11/2016

Non-Publication Request: No

Early Publication Request: No

page 1 of 3

Title

MOBILE MALWARE DETECTION AND USER NOTIFICATION

Preliminary Class

726

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 Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/617,787				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)	OR	RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	600			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720			
TOTAL CLAIMS (37 CFR 1.16(i))	31 minus 20 =	* 11			OR	x 80 =	880			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	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	2480			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	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.										



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.
14/617,787	02/09/2015	Rainer Baeder	FORT-012700	1008
64128 7590 11/18/2016 MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP FINANCIAL PLAZA AT UNION SQUARE 225 UNION BOULEVARD, SUITE 150 LAKEWOOD, CO 80228			EXAMINER RUPRECHT, CHRISTOPHER S	
			ART UNIT 2494	PAPER NUMBER
			NOTIFICATION DATE 11/18/2016	DELIVERY MODE ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesantis@hdciplaw.com
docket@hdciplaw.com

Office Action Summary

Application No.
14/617,787

Applicant(s)
BAEDER, RAINER

Examiner
CHRISTOPHER RUPRECHT

Art Unit
2494

AIA (First Inventor to File)
Status
Yes

-- 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 16 August 2016.
☐ 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) 1-31 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☒ Claim(s) 1-31 is/are rejected.

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

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

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

Application Papers

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a) ☐ All b) ☐ Some** c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

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

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

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

4) ☐ Other: ____.

Art Unit: 2496

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

1. This office action is in response to the communication filed on 08/16/2016.
2. Claims 1-31 are pending, and have been examined on the merits. Claims 1, 2, 6, 9, 10, 18-22, 24, and 27-31 are currently amended. No new matter has been added.

Response to Arguments

Regarding Claim Rejections Under 35 USC 102 and 103

3. Claims 1-6, 11-20, and 22-31 were previously rejected under 35 USC 102(a)(1) as being anticipated by Gupta (US 2014/0189861). Applicant's arguments on pages 10-12 of the Reply accompanying the current amendment regarding the previous 35 USC 102 rejection of independent Claims 1 and 18 based on Gupta alone have been considered, and have been determined by Examiner to be persuasive. Gupta does not clearly teach that a "malware reporting/notification message" is necessarily sent to the user/subscriber of the portable computing device "in real-time", per se. Furthermore, Gupta is also silent as to specifying a "timeframe" (i.e., a predetermined time period/window/limit) by which the user/subscriber must perform appropriate "remedial actions", as indicated by the notification message. **Accordingly, the previous 35 USC 102(a)(1) rejection of Claims 1-6, 11-20, and 22-31 based on Gupta alone is hereby withdrawn.**

Art Unit: 2496

4. However, the current amendments to independent Claims 1 and 18 have incorporated various new features, partially from dependent Claims 10 and 21 at least conceptually (i.e., which previously recited that the malware reporting/notification message "includes information regarding the malware event and giving the user a set time by which to address the malware event"), but more fully from previously unclaimed details supported in the specification. Specifically, none of the claims previously discussed the malware reporting/notification message including any "information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information" (i.e., this is not the same thing as "information regarding the malware event") nor that it "specifies a timeframe within which the user must perform the remedial action or risk deactivation of service provided to the portable computing device" (i.e., this is not the same thing as "giving the user a set time by which to address the malware event"). Therefore, the new features of currently amended independent Claims 1 and 18 are subject to a substantially different and narrower scope of interpretation as compared to the related phrase that was previously contained in dependent Claims 10 and 21 (which was subject to a significantly broader interpretation under the broadest reasonable interpretation).

5. Applicant's arguments have been considered but are rendered moot in view of the new grounds of rejection set forth below, as necessitated by Applicant's current amendments to the independent claims. **Accordingly, pending Claims 1-31 remain rejected under 35 USC 103, based on a combination of the previously cited prior**

Art Unit: 2496

art reference Gupta with two new prior art references that were discovered in the updated search that was necessitated by Applicant's narrowing amendment to independent Claims 1 and 18.

Regarding Claim Objections

6. Claims 2, 9, 10, 18-21, 24, 27, and 31 were previously objected to for various minor informalities. Applicant's current amendments to these claims substantially incorporate Examiner's suggestions provided in the previous office action for addressing these issues. **Accordingly, the previous objections to Claims 2, 9, 10, 18-21, 24, 27, and 31 are hereby withdrawn.**

Claim Rejections - 35 USC § 103

7. 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, 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.

8. **Claims 1-31 are rejected under 35 USC 103 as being unpatentable over Gupta et al. (US 2014/0189861), in view of Rieschick et al. (US 2012/0233656), and in further view of Gleichauf et al. (US 9,436,820).**

Regarding Claims 1 and 18: (Independent)

Gupta teaches **A method** (Gupta, see the previously cited excerpts from paragraphs [0019, 0032]) **comprising:**

detecting, by a malware detection gateway device associated with a mobile service provider network, a malware event based on a data stream transmitted to or from a portable computing device (Gupta, see the previously cited excerpts from paragraphs [0020, 0028-0030, 0032, 0041-0042, 0054-0055, 0065, 0067], which were not contested by Applicant in the “Reply”)
communicating with a packet data network via the mobile service provider network (Gupta, see Fig. 1 and the previously cited excerpts from paragraphs [0013, 0015-0016, 0018, 0020-0021, 0025, 0037, 0045], which were not contested by Applicant in the “Reply”); **and**

causing a malware reporting/notification message to be send to a user of the portable computing device... (Gupta, see the previously cited excerpts from paragraphs [0033, 0035, 0056, 0059, 0066]. However, as indicated in the “Response to Arguments” section above, Gupta does not necessarily clearly teach that this malware reporting/notification message is sent to the user of the portable computing device “in real-time”, per se, as currently amended), **by sending, by the malware detection gateway device, a malware indicating message to a lookup device, wherein the malware indicating message comprises an Internet Protocol (IP) address of the portable computing device** (Gupta, see the previously cited excerpts from paragraphs [0029-0033, 0041-0042, 0051, 0055-0056, 0065-0067], which were not contested by Applicant in the “Reply”),

wherein the malware reporting/notification message (i) includes information regarding...the detected malware event... (Gupta, paragraphs [0033, 0035, 0056, 0059, 0066] are relevant to the mobile service provider taking immediate

“remediation actions” (but not necessarily the user of the portable computing device performing a remedial action, as indicated in the notification message), generally providing users with a notification message regarding a “detected malware event” (i.e., in order to “educate” the users/owners of subscriber devices about their particular behavior in the network, via the generation and sharing of customer-specific behavior reports), and generally sending an “alert” to one or more email addresses, phone numbers, computers, or other devices. However, Gupta does not provide a clear express teaching of this entire claim limitation as a whole).

As indicated in the previous office action, Gupta teaches a “lookup device”/“user lookup module” (i.e., “network threat behavior and analysis engine 6” including “correlation module 36”) comprising a “lookup table” (i.e., a “subscriber table”, a “mapping table 39” stored in “database 38”) that stores “network addresses” that are associated with “portable computing devices” (i.e., “IP addresses” that are assigned to “subscriber devices 12” in order to serve as “unique identifiers” thereof in the network) and that are “mapped”/“linked” to corresponding “subscriber device information” (e.g., “Mobile Station International Subscriber Directory Number” (MSISDN), “International Mobile Subscriber Identity” (IMSI), “International Mobile Equipment Identity” (IMEI), and “access point name” (APN), for the purpose of enabling mobile network operators/administrators to “identify” the corresponding “users” (i.e., “subscribers”, “customers”) that are associated with the respective “portable computing devices” (i.e., “subscriber devices 12”), such that they may be notified of their network behavior and any corresponding malware events that were detected in network data traffic (i.e., so that they may then perform some sort of remediation in order to remove the malware infection, or otherwise address the detected malware event as appropriate).

But Gupta does not expressly teach each and every feature of Claim 1,

which as currently amended now further includes the following additional details: **...causing a malware reporting/notification message to be sent to a user of the portable computing device in real-time..., wherein the malware reporting/notification message (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information and (ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of service provided to the portable computing device.**

However, in the same field of endeavor (i.e., methods, systems and devices for the detection and prevention of malware within a network), Rieschick teaches **A method comprising:**

detecting, by a malware detection gateway device associated with a mobile service provider network (Rieschick, see paragraphs [0035, 0038, 0041-0042, 0045] regarding a malware detection “gateway device” associated with a “mobile service provider network”, which is coupled to a “policy management system 116”), a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the mobile service provider network (Rieschick, “receiving from one or more communication system control network components data flow parameters identifying characteristics of a data flow, performing a detection method to determine if the data flow carries malicious content...a communication system gateway configured to control the flow of packet-based data between a wireless device and an external network...The data flow may originate from a wireless device or an Internet server,” paragraph [0006]; “a comprehensive security solution for detecting and preventing malware from within a mobile data network...monitor network traffic for suspicious content or activities to detect malware and block suspicious data flows from within the network,” paragraph [0027]; “detect transmissions of known and unknown malware

in real time as the network patterns emerge...machine learning mechanisms to enable the malware protection system to learn about malware-generated transmissions and recognize malware patterns as they develop...tracking or correlating network activity levels of recognized threats...store...malware detection (e.g., patterns in network traffic that occurred while a malware event was underway)...information...used by the malware protection system for the detection...of...malware events...Malware threats may be identified using any suitable mechanism," paragraph [0029]; "detect spam by recognizing network traffic with certain characteristics, which may include destination information, protocols, and/or payload content...may detect denial of service attacks by recognizing rapid increases in traffic addressed to a single or related destination from multiple sources," paragraph [0031]; "The gateway/PCEF 114 may contain a deep packet inspection (DPI) component...configured to obtain additional application-level information about a particular IP data flow," paragraph [0038]; "The malware protection system 126 may maintain a repository of known security risks, gather real-time information regarding emerging security/malware threats, identify security malware threats by monitoring traffic within the communication network 100," paragraph [0042]; "The policy management system 116 may identify appropriate policy rules for a given situation and send the identified policy rules to the gateway/PCEF 114 for enforcement...The policy rules may further govern whether specific IP data flows should be "blocked," "allowed" or "allowed with constraints," based on current and potential security risks/malware threats," paragraph [0046]; "The policy management system 116...to identify potential security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference...identified security risks (e.g., known virus, irregular usage patterns, etc.)...generate and/or select one or more rules or rule groups, which are pushed to the gateway/PCEF 114 for enforcement," paragraph [0047]; "gateway/PCEF may receive a data flow originating from, or destined for, a wireless device...may examine the data flows and/or the network traffic, identify key characteristics of the

*data flows and/or network traffic, generate parameters based on the key characteristics and send the generated parameters to a policy management system for analysis...may receive one or more policy rules from the policy management system...may use the received policy rules to enforce the various policies...such as blocking, restricting, or allowing the data flow to be sent to, or received from, a wireless device,” paragraph [0054]; “the policy management system may receive parameters generated by the gateway/PCEF...may use the received parameters to determine if the data flows carry content (e.g., malware) that poses a security risk to network and/or wireless devices...may use the parameters to perform pattern matching detection methods or observed behavior detection methods to determine if the data flow carries malicious content or is otherwise a security risk...may retrieve information from a local memory and/or request/receive information from external memories/systems/servers...that may be used to determine if the data flows carry content (e.g., malware) associated with a potential or known security risk...may generate/select policy rules based on determining the data flows carry content that poses a “known risk”, a “potential risk,”...may send the generated/selected policy rules to the gateway/PCEF for enforcement,” paragraph [0055]; also see paragraphs [0008, 0022, 0024, 0028, 0041, 0048, 0050-0052, 0057-0058, 0060, 0069] generally); **and***

causing a malware reporting/notification message to be sent to a user of the portable computing device in real-time (Rieschick, “detect transmissions of known and unknown malware in real time as the network patterns emerge...alert wireless device users of detected malware...warn targets of an attack,” paragraph [0029]; “push client software capable of exchanging malware and security information with a control network to wireless devices...may include...alerts generated by the system,” paragraph [0030]; “send detection and prevention information to...wireless devices...in real time,” paragraph [0032]; “a user repository 122. The policy management system 116 may communicate with a malware protection system 126 and a notification server 128 in a network (External

Network) 130...The notification server 128 may be configured to...send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR systems)...depending on the user's preferences and/or mobile device type. Messages may be sent through the Internet 107 or the access gateway 110...the notification server 128 may send messages to a client application running on the mobile devices 102," paragraph [0039]; also see paragraph [0040] generally; "The mobile device formats may be defined by configuration or determined in real time by the policy control system 116, or by the malware protection system 126 based on information received in real time from the policy control system 116," paragraph [0042]; "telecommunications network operators and their customers may customize responses to malware events, which may be implemented automatically and in real time, consistent with the type of threat and how the network operator and/or customer prefers to respond," paragraph [0070]; "the policy management system may access the user preference parameters to determine that the correct course of action (i.e., the correct rule) for the gateway/PCEF upon the detection of...malware is to send an alert message to the wireless device," paragraph [0072]; "interacting with the user (e.g., via SMS messages sent through the notification server 126, etc.) to determine his/her preferences in real-time...a wireless device user may upload user preference parameters to the user repository that instructs the policy management system to send an alert to the user's wireless device warning of potential risks," paragraph [0074]; "a message is sent warning of potential malware," paragraph [0079]),

by sending, by the malware detection gateway device, a malware indicating message to a lookup device, wherein the malware indicating message comprises an Internet Protocol (IP) address of the portable computing device (Rieschick, "alert telecommunications network operators of detected malware so they can take corrective actions and/or warn targets of an attack...store user-specific malware detection (e.g., patterns in network traffic that occurred while a

malware event was underway) and prevention information (e.g., countermeasures that proved effective in responding to a malware event)...map specific malware threats identified to users of the network. Malware threats may be identified using any suitable mechanism, including the use of IP addresses," paragraph [0029]; "send detection...information to telecommunications network operators...and/or malware systems in real time," paragraph [0032]; "The SGW 28 stores information about the data (e.g., parameters of the IP bearer service, network internal routing information, etc.) and forwards user data packets to a policy control enforcement function (PCEF) and/or packet data network gateway (PGW) 32. The PCEF/PGW 32 sends signaling information (control plane) to a policy control rules function 34. The PCRF 34 accesses subscriber data bases, creates a set of intelligent policy rules...and sends the intelligent policy rules to the PCEF/PGW 32 for enforcement...implements the policy rules to control...services and flows being communicated between the service network 36 and the end users," paragraph [0035]; "The gateway/PCEF 114 may contain a deep packet inspection (DPI) component...configured to obtain additional application-level information about a particular IP data flow and provide the information to other components in the PCC network 112," paragraph [0038]; "The policy and charging control network 112 may also include a policy management system 116...and a user repository 122. The policy management system 116 may communicate with a malware protection system 126 and a notification server 128 in a network (External Network) 130...The notification server 128 may be configured to receive requests from the policy management system 116 (e.g., PCRF) and send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems," paragraph [0039]; "the user repository 122 may include a subscriber profile repository (SPR)," paragraph [0044]; "the policy management system 116 may communicate with the user repository 122...may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific

information, such as details of a user's subscription to malware prevention services and historical details of a user's exposure to specific malware threats...may use the information stored by the user repository 122...to identify potential security risks/malware threats and user preferences for responding to identified security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference," paragraph [0047]; "the policy management system may extract...IP address information...from the received parameters," paragraph [0057]; "the policy management system may compare the IP address information with a list of known offender IP addresses to determine if the IP data flow originates from, or is destined for, a mobile device that is compromised (e.g., infected with malware, a virus, etc.) or blacklisted (e.g., known to intentionally engage in malicious activities). If the policy management system determines that the IP address information is associated with an IP address in the list of known offender IP addresses...generate policy rules that block or restrict the data flow and push the generated rules to the gateway/PCEF for enforcement...generate an "allow with constraints" rule upon determining that the IP data flow carries content originating from, or destined for, a mobile device that is compromised or blacklisted," paragraph [0061]; "IP level monitoring operations may include monitoring requests to a specific port 80 of a specific IP address," paragraph [0066]; "the policy management system may perform quarantining operations by storing details of IP data flows, aggregated details of the IP data flows, or sequestering the actual content of the IP data flows, that were allowed, constrained, or blocked. The policy management system may store source information, destination information and time information for each IP data flow that is constrained...may track the number of IP data flows containing in infected binaries within a predetermined time period...and store the number value in a memory...may also store emails deemed to be spam. This information may be stored such that a wireless device user whose mobile device is associated with these IP data flows may subsequently view the quarantining details," paragraph [0073]; "The policy management system may,

upon determining that an IP data flow is associated with a malware threat, notify the malware protection system of the wireless device's identity and the detected malware," paragraph [0077]; *"The policy management system may exchange information with...a user repository,"* paragraph [0078]; also see paragraphs [0043, 0046, 0070, 0072, 0074] generally).

Thus, Rieschick teaches or otherwise suggests in an obvious manner that a user's "portable computing device" that is communicating in the network may be identified based on its associated "IP address", which may then be used as a basis for mapping to corresponding stored "user-specific information" (e.g., a user ID, a user's email address and/or cellular telephone number, user behavior and malware-related history in the network, user preferences for responding to detected malware threats, etc.) for enabling the transmission of malware notification messages to the user for timely malware remediation purposes.

wherein the malware reporting/notification message (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information...the user must perform the remedial action or risk deactivation of service provided to the portable computing device (Rieschick, "generating

restrictive policy rules in response to determining the data flow carries malicious content, and pushing the generated policy rules to a communication system gateway configured to control, the flow of packet-based data between a wireless device and an external network...instruct the gateway to block the data flow and/or to block future data flows originating from the wireless device," paragraph [0006]; *"enable defensive and ameliorative actions, such as modifying the transmissions of the malware or transmission generated by the malware...may prevent the transmission of malware once it has been detected...may alert wireless device users of detected malware...take corrective actions and/or warn targets of an*

attack...store user-specific...prevention information (e.g., countermeasures that proved effective in responding to a malware event), which may be used by the malware protection system for the detection and prevention of future malware events,” paragraph [0029]; “push client software capable of exchanging malware and security information with a control network to wireless devices...may include report details generated by the client, alerts generated by the system, instructions from the system to the client that relate to a specific threat to the client, and/or instructions that instruct the wireless device to change its behavior,” paragraph [0030]; “send detection and prevention information to...wireless devices...in real time,” paragraph [0032]; “The notification server 128 may be configured to...send messages to mobile devices 102 using various technologies mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems...depending on the user's preferences and/or mobile device type...may send messages to a client application running on the mobile devices 102 (e.g., via the Internet 107, access gateway 110, etc.),” paragraph [0039]; “The malware protection system 126 may...generate security/malware threat countermeasures...may include malware removal software and/or malware repair software...in a format specific to each mobile device 102 type. The mobile device formats may be defined by configuration determined in real time by the policy control system 116, or by the malware protection system 126 based on information received in real time from the policy control system 116,” paragraph [0042]; “The policy management system 116 may also communicate with external systems 155, such as a malware protection system 126 and a notification server 128...the malware protection system 126 may maintain a repository of known malware threats, gather information regarding emerging malware threats, identify current and potential malware threats and generate malware threat counter-measures, malware removal software and/or malware repair software to neutralize the security threats,” paragraph [0048]; “the policy management system may access information stored in a user repository...in a

control network to identify and neutralize security risks that cannot be identified or neutralized by systems that do not have access to user/charging information,” paragraph [0064]; also see paragraphs [0070-0071] generally; *“the policy management system may access the user preference parameters to determine that the correct course of action (i.e., the correct rule) for the gateway/PCEF upon the detection of low-risk malware is to send an alert message to the wireless device without blocking the IP data flow. Likewise, the user preference parameters may be used by the policy management system to generate rules that instruct the gateway/PCEF to block the current IP data flow and all future IP data flows until the malware has been manually removed from the mobile device,”* paragraph [0072]; *“the policy management system may perform quarantining operations by storing details of IP data flows...that were allowed, constrained, or blocked...This information may be stored such that a wireless device user whose mobile device is associated with these IP data flows may subsequently view the quarantining details,”* paragraph [0073]; *“interacting with the user (e.g., via SMS messages sent through the notification server 126, etc.) to determine his/her preferences in real-time...a wireless device user may upload user preference parameters to the user repository that instructs the policy management system to send an alert to the user’s wireless device warning of potential risks,”* paragraph [0074]; *“a malware prevention and removal client (MPRC) software application may be pushed to the wireless devices...The malware protection system may then update, or instruct, the MPRC to take preventative, recovery, or removal actions specific to the wireless device type or type value and the detected malware threat. For example, the malware protection system may instruct the MPRC to disable the wireless device’s data capabilities and/or isolate the mobile device from the mobile data network until the malware is removed or is otherwise no longer a threat,”* paragraph [0077]; *“malware is detected and/or removed from the user’s wireless device,”* paragraph [0078]; *“a message is sent warning of potential malware,”* paragraph [0079])...

The claimed phrase *“remedial action that can be taken by the user to*

neutralize malware associated with the detected malware event" is interpreted based on the disclosure in paragraphs [0042, 0048, 0051-0052, 0060, 0067] of Applicant's specification. Rieschick teaches substantially similar equivalent embodiments based on this disclosure.

Rieschick does not expressly teach that the "malware reporting/notification message" further ...**(ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of service provided to the portable computing device.**

The claimed phrase "timeframe within which the user must perform the remedial action" is interpreted based on the disclosure in paragraphs [0021, 0040, 0051, 0067] of Applicant's specification. Rieschick does not teach substantially similar equivalent embodiments based on this disclosure. Rather, Rieschick is silent as to specifying a predetermined "timeframe" (i.e., a timer or grace period) for performing the required remedial action, per se. Instead, the teachings of Rieschick from paragraphs [0072, 0077] above are somewhat different that this final limitation of the independent claims, in that the system may deactivate the user's/device's service until the remedial action is performed (at which time service may then be re-activated), as opposed to imposing a pre-determined time limit for performing the remedial action, and then only deactivating the service in response to exceeding the time limit. Rieschick also generally teaches in paragraph [0046] that the "policy management system 116" identifies policy rules that govern how long the subscriber may access certain services (e.g., 15 minutes at a time, a total of two hours, etc.), and that the policy rules further govern whether specific IP data flows should be "blocked," allowed" or "allowed with constraints" based on current and potential security risks/malware threats. However, again this is distinguishable from the claimed limitation regarding specifying a timeframe for performing suggested remedial actions based on

the remediation information provided in a malware notification message.

Additionally, in the same field of endeavor (i.e., detecting malware and performing remediation thereof, and controlling access to resources in a network), Gleichauf teaches **A method comprising:**

detecting, by a malware detection gateway device associated with a mobile service provider network, a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the mobile service provider network; and causing a malware reporting/notification message to be sent to a user of the portable computing device in real-time (Gleichauf, teaches the “real-time” detection and transmission of reporting/notification messages regarding “malware events” via communications between a “user device”/“computerized device 22”, a “data communications device 26”, and a “policy server 28”, based on a “challenge-response sequence” and corresponding analysis of “security posture credentials” associated with a current configuration and/or security state of the user’s portable computing device, for the purpose of reducing the opportunities for injecting malware into a network. Devices that are detected to be out of compliance with network admission/access/security policies, based on the security posture credentials check, may be redirected to a remediation server via the malware reporting/notification message in order to perform certain remedial actions for neutralizing the malware threat, prior to permitting access to restricted network resources. For specific implementation details and discussion, see the following excerpts: Col. 3, lines 28-49; Col. 4, lines 21-40, 50-60; Col. 5, lines 17-26; Col. 8, lines 1-31; Col. 8, line 38 – Col. 9, line 5; Col. 9, lines 29-45; Col. 10, lines 6-44; Col. 12, lines 4-21; Col. 15, line 55 – Col. 16, line 6; Col. 23, lines 36-44),

...wherein the malware reporting/notification message (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to

the information (**Gleichauf**, teaches that the “malware reporting/notification message” includes “information regarding a remedial action that can be taken by the user to neutralize the malware” associated with the detected malware event or a “link to the information” (i.e., the “notifications” include the results of the security posture credential check, any “remediation actions” that need to be performed and an informational message to be displayed to the user, a redirection message including a clickable IP address/URL/link to a remediation server, etc.). The user then connects their computing device to the remediation server on the quarantine network in response to the notification message, which reconfigures, updates or provides up-to-date patches to the OS and/or anti-virus applications (and corresponding most current versions of virus signatures files) associated with the device in order to become compliant with the network security policies and thereby neutralize the malware threat to the device, the network, and the network resources. For specific implementation details and discussion, see the following excerpts: Col. 4, lines 21-27, 50-63; Col. 5, lines 1-11; Col. 5, lines 17-29; Col. 9, lines 43-50; Col. 10, lines 39-44; Col. 16, lines 7-21, 29-33; Col. 18, lines 22-25; Col. 20, line 17 – Col. 21, line 23; Col. 23, line 56 - Col. 24, line 5)...

Gleichauf also generally teaches ...**a timeframe within which the user must perform the remedial action or risk deactivation of service provided to the portable computing device** (**Gleichauf**, see Col. 4, lines 19-40 (i.e., devices that are compliant with the network admission policies are given full network access, devices that are mildly out of compliance may be issued a warning, devices that are significantly out of compliance may be placed on an isolated/quarantine network segment where they can be brought into compliance by performing the remedial actions, and devices that violate core admission requirements may be denied network access entirely. This is a policy decision based on “periodic” performance of the “security posture credential” analysis associated with the user’s portable computing device, thereby limiting at-risk or vulnerable computerized devices from accessing the protected network resources and minimizing the risk that they will

become infected with malware); "The device should be admitted into the original network if the remediation process was successful. Otherwise the device will be again identified as being at some level of non-compliance and the appropriate response will be invoked by the policy server," Col. 5, lines 11-16; "Once the computer device has completed the remediation process, the computer device can attempt to re-enter the original network. This may be achieved by the computer device transmitting a message to the data communications device to request that the posture of the device be re-validated, and/or the data communications device may periodically query the computer device for a posture update...called "posture update query". When the posture agent responds to a posture update query in a way that indicates that the posture has been updated, the data communications [device] initiates a fresh challenge-response sequence to enable the policy server to re-assess the posture credentials and apply new admission to the data communications device. The posture update query mechanism is used to detect any change in posture of the computer device. Changes may be due to the remediation process, other software updates processes, user action, or infection by some type of malware...the data communications device may periodically transmit the posture update query message to the posture agent...The status query mechanism is a simple authenticated challenge-response mechanism used to determine whether the posture on the computer device has changed...If the status query fails, e.g., because the posture agent responds with an error, the posture agent does not respond at all or the posture agent indicates that the posture agent has changed, the data communications device attempts the full challenge-response sequence to enable the policy server to re-assess the posture credentials and apply a new access policy to the data communications device," Col. 5, lines 30-67; "The posture agent is also responsible for determining whether the posture of the computer device 22 has changed by learning of any changes from the posture plug-ins 32 through the posture plug-in API. The posture agent is responsible for answering the periodic posture update query from the data communications device

between the full posture challenge-response sequences," Col. 9, lines 50-56; see Col. 10, lines 33-39 and Col. 12, lines 4-21 (i.e., regarding either allowing or denying network/resource access to the user's portable computing device based on the periodic analysis of the "security posture credentials" and corresponding configuration and/or security state of the user's portable computing device, wherein vulnerable devices that are not configured with the latest anti-virus software updates are denied access in order to prevent the network/resources from becoming infected with malware); see Col. 14, lines 16-54 (i.e., regarding the risk of "deactivation of service provided to the portable computing device", such as when "remedial actions" including downloading updated anti-virus applications or virus definition files or correcting a discrepancy between the posture credentials of the user device and the accepted credential set of the policy server have not been performed in a timely manner); "the data communications device 26 restricts the computerized device's 22 access to resources 25 within the network 24 based upon instructions 48 provided by the policy server 28. The data communications device 26 also works in conjunction with the policy server 28 to upgrade or "fix" applications associated with the user device 22 when the policy server 28 detects that the user device 22 is vulnerable or susceptible to a virus or has other configuration problems," Col. 15, lines 36-44; "an operator or the remediation process can upgrade certain security applications associated with the device so that a non-compliant device now becomes compliant to security policy (e.g., updates the anti-virus signature file to the most current version)...with respect to system 20, the user device 22 is no longer a risk to the network and should be given access to network resources 25 in network 24," Col. 16, lines 29-33, 40-43; "the data communications device 26 periodically polls the user device 22 using the posture update query. In the case where the data communications device 26 detects a change in the state of the user device 22, the data communications device 26 attempts to re-authorize the posture of user device 22 as explained in FIG. 1 (i.e., triggers the re-start of the full system process as described in FIG. 1).

If this attempt is unsuccessful, the data communications device may remove all access permissions for user device 22 to minimize the risk of virus or malicious content introduction by the user device 22 to the network 24,” Col. 16, lines 48-59; “the data communications device 26 transmits a posture update query to the computerized device 22 after expiration of a time period...the data communications device 26 includes a timer 70...when the data communications device 26 applies an access instruction 48 for the user device 22, provision of such access initiates operation of the timer 70 such that a timer counts from a start time to a preset end time. After expiration of a preset time period (e.g., the time period between the end time and the start time), the timer 70 causes the data communications device 26 to transmit a posture update query to the computerized device 22,” Col. 16, line 66 – Col. 17, line 10; “the data communications device detects a change in posture associated with the computerized device 22 based upon a response to the posture update query. The data communications device 26 interprets either an actual response or a lack of a response from the computerized device 22 to determine the state of the computerized device 22...Based upon the non-response, the data communications device 26 reduces network access privileges or terminates the connection between the user device 22 and the network resource 25 to reduce the risk of reception or transmission, by the network resources 25 of an unauthorized application from a “vulnerable” user device or a device susceptible to a virus. In this manner, periodic posture checking can be performed,” Col. 17, lines 22-29, 52-59; also see Col. 17, line 63 – Col. 18, line 18 for another example (i.e., when an operator disables or reconfigures an anti-virus application, and the response to the next periodic “posture update query” indicates the change in configuration of the OS and anti-virus application, which may also cause reduced access privileges or terminating the connection to reduce the risk of spreading a malware infection to the network/resources); also see Col. 18, lines 22-45 for another example (i.e., when the user device was not deemed by the policy server to be compliance with the network security policies and is given restricted access to network resources

sufficient only to remediate itself, wherein once remediation has completed successfully the response to the next periodic "posture update query" indicates the corresponding change in configuration of the OS and/or anti-virus application (i.e., that the remedial action was indeed performed within that "timeframe") which may then cause increased or normal network/resource access privileges to be enabled for the user's portable computing device); "the data communications device 26 periodically re-executes the sequence described with respect to FIG. 1 based on expiration of a preset time period. A timer associated with the data communications device 26...initiates measurement of a time period after the data communication device 26 receives the access request 40 from the computerized device 22...after a timer reaches the preset time period, the data communications device transmits to the computerized device 22 a challenge request 42, as part of the re-executed challenge response sequence of FIG. 1," Col. 19, lines 4-15; "the policy server 28 transmits the network admission or access instruction 48 to the data communications device 26...directs the data communications device to either allow some level of network access or deny the computerized device 22 access (e.g., restrict access of the computerized device 22) to the resources 25 within the network 24...based upon the analysis, the policy server 28 fails to detect the presence of, proper configuration, or timely execution of the anti-virus application from the particular manufacturer within the accepted credentials set 46...the policy server 28 transmits a network admission instruction 48 to the data communications device 26 that directs the data communications device to restrict or reject communications from the user device 22 to the resources 25 within the network...the policy server 28 detects the real-time security posture or security state of a user device 22 (e.g., as indicated by the posture credentials 32) prior to providing the user device 22 with access to the network resources 25. By detecting the real-time security state of the user device 22, the policy server 28 aids in minimizing "vulnerable" user device 22 (e.g., user devices 22 that are not configured with anti-virus or up-to-date anti-virus applications) from accessing the

network 24. As such, the policy server 28 aids in minimizing the risk that the network 24 or resources 25 become "infected" with malware carried by the "vulnerable" user device 22," Col. 22, lines 24-30, 39-59).

At the time of the effective filing date of the claimed invention, one having ordinary skill in the art would have recognized to modify the "system and method for correlating network information with subscriber information in a mobile network environment" of Gupta, and the "methods, systems and devices for the detection and prevention of malware within a network" of Rieschick, with the "controlling access to resources in a network" of Gleichauf. The motivation for such a combination is that once a portable computing device that is connected to a network and communicates with other devices has been infected with malware, that malware can quickly propagate throughout the network infecting other devices as well as having a detrimental effect on the network itself. Therefore, there is a significant need to perform the timely remediation of such malware before it has a chance to spread, and specifying a "timeframe" for a user/portable computing device to perform remediation of the detected malware, which if exceeded causes "deactivation" of network service being provided to the portable computing device, ensures that either the malware will indeed be remediated within that predetermined timeframe or else that the device will be prevented from connecting to the network and communicating with other devices so as to enable the malware to spread throughout the network and infect other devices in case remediation is not performed in a timely manner. The rationale for not immediately "deactivating" network service provided to the user's portable computing device, and instead instituting a limited "grace period" for performing malware remedial action(s), is that the user/portable computing device might need continued access to the network and its resources in order to perform such remediation operations (e.g., downloading updating anti-virus software, receiving an indication of new

configuration settings, contacting a remediation server to receive further instructions regarding neutralizing the malware, etc.). Thus, the combination provides enhanced security and the timely performance of malware remediation in order to protect the network and its devices by reliably ensuring that any detected malware has a limited opportunity to spread throughout the network and infect other devices based on this “timeframe”.

However, Gleichauf does not *expressly* teach ...**wherein the malware reporting/notification message...(ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of service provided to the portable computing device.** (*emphasis added*). Although Gleichauf does clearly teach such a “timeframe” in general as indicated by the excerpts above, it does not necessarily indicate that its disclosed “timer” or its corresponding “preset end time” (i.e., indicating the “expiration” of the timer), or else an indication of how often the “periodic” polling of the user’s portable computing device with a “posture update query message” will be performed, is actually included directly in the “malware notification message” itself, per se.

Nevertheless, one having ordinary skill in the art at the time of the effective filing date of the claimed invention would have considered it to be trivial, straightforward, and obvious to impose some sort of “timeframe” or “grace period” (e.g., 10 minutes, 1 hour, 1 day, etc.) for the user to perform the one or more “remedial action(s)” that are included in the malware notification message in order to effectively “neutralize malware” that has been detected, and actually providing a clear indication of that specified “timeframe” directly in the malware notification message itself in order to provide adequate notice to the user regarding that timeframe, such that the continued providing of service to the user/mobile device would only then be denied/blocked if that time limit is exceeded without the corresponding remediation being performed for the mobile device by the user. Gleichauf teaches that failure

to timely remediate malware based on a notification message sent to a user of a portable computing device may result in the denial of continued access to network services (e.g., see Col. 22, lines 38-47), and that the security posture is periodically re-checked upon expiration of a timer (e.g., see Col. 19, lines 4-14). Given the teachings of Gupta that the user should be notified of a detected malware event and information regarding any corresponding remedial actions, and further coupled with the teachings of Rieschick that such notifications should be sent to the user "in real time" upon malware detection, such a person would have considered it to be obvious to have included the time limit of Gleichauf directly into the user malware notification messages of Gupta and/or Rieschick. The rationale for specifying and permitting such a timeframe or grace period, as opposed to immediately deactivating service upon malware detection, is that the user's device may need to have continued access to the network services in order to actually perform the remedial action(s) indicated in the malware notification message (e.g., download updated anti-virus software, determine new configuration settings, contact a remediation server to receive further instructions regarding neutralizing the malware, etc.). Furthermore, the rationale for notifying the user of this "timeframe" directly in the malware notification message itself is so that the user will know how long they have to actually perform the suggested remedial action(s) before their service will be deactivated in the case of failed remediation. An additional obviousness motivation for specifying such a timeframe in the malware notification message itself is that the actual amount of time required to perform particular remedial action(s) may vary, and the actual risk of harm to the device itself, other network devices, or the network in general may also vary, such that users should be given less time to perform remedial actions that may be performed relatively quickly or where the threat level posed by the particular malware detected is high, whereas users should be given more time to

perform remedial actions that may take longer to perform or where the threat level posed by the particular malware detected is low. Similarly, the specified “timeframe” for performing suggested remedial action(s) may be dynamically adjusted over time as malware is detected and remediated (or not remediated) and corresponding network-side responses and/or penalties to the user/device may be escalated or de-escalated depending on the timely performance of remediation or lack thereof (i.e., such as from a warning, to quarantining, and finally to full termination of service upon repeated or continued failure to remediate detected malware in a timely manner), such that users whose devices are frequently detected to be infected with malware or otherwise fail to timely perform remediation upon a first notification are given less time to perform remediation upon subsequent notifications in order to reduce the risk to the network and other devices, whereas users whose devices are infrequently detected to be infected with malware or otherwise do indeed timely perform remediation upon a first notification are given more time to perform remediation upon subsequent notifications since they may be considered less of a risk to the network and other devices. Thus, there are a wide variety of potential reasons that would occur to one having ordinary skill in the art for including a “timeframe” for performing remedial action(s) directly in the malware notification message itself that is delivered to the user of the portable computing device.

Similarly as to Claim 18, Gupta as further modified by Rieschick and Gleichauf in the rejection of Claim 1 above teaches **A malware detection system operable within a mobile service provider network comprising: one or more processors; a communication interface device; and one or more internal data storage devices operatively coupled to the one or more processors and storing instructions (Gupta**, see Figs. 1, 2, and 6, as well as the previously cited excerpts from paragraphs [0019, 0032, 0068-0076], which were not contested by Applicant in the “Reply”. **Rieschick**, also teaches a malware detection system

Art Unit: 2496

operable within a mobile service provider network comprising one or more processors, a communication interface device, and one or more internal data storage devices storing instructions coupled to the processor(s)) **representing:**

a malware detection module, which when executed by the one or more processors, detects a malware event associated with a data stream originating from or directed to a portable computing device communicating with a packet data network via the mobile service provider network (Gupta, see Fig. 1 and the previously cited excerpts from paragraphs [0013, 0015-0016, 0018, 0020-0021, 0025, 0028-0030, 0032, 0037, 0041-0042, 0045, 0054-0055, 0065, 0067], which were not contested by Applicant in the “Reply”. Rieschick, see the rejection of Claim 1 above. Gleichauf, see the rejection of Claim 1 above);

a user lookup module, which when executed by the one or more processors, identifies a user corresponding to the portable computing device based on a lookup table and a unique identifier associated with the portable computing device (Gupta, see the previously cited excerpts from paragraphs [0030-0033, 0041-0042, 0051, 0056, 0065-0067], which were not contested by Applicant in the “Reply”. Rieschick, see the rejection of Claim 1 above, wherein Rieschick teaches a “user lookup module” that “identifies a user corresponding to the portable computing device based on a lookup table and a unique identifier associated with the portable computing device” (e.g., which maps an “IP address” to a corresponding “user ID” and other user-specific information));

a malware-indicating message module, which when executed by the one or more processors, queries the user lookup module by providing information relating to the detected malware event and the unique identifier (Gupta, see the previously cited excerpts from paragraphs [0029-0030, 0032, 0055, 0065, 0067]. Rieschick, see the rejection of Claim 1 above, wherein Rieschick teaches a “malware-indicating message module” that “queries the user lookup module by providing information relating to the detected malware event and the unique

Art Unit: 2496

identifier" (e.g., so that the "user lookup module" can map the "IP address" to the corresponding "user ID")); **and**

a malware reporting module, which when executed by the one or more processors, provides a notification to the user in real-time regarding the detected malware event, wherein the notification (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information (**Gupta**, see the rejection of Claim 1 above for citations and corresponding discussion (However, Gupta does not necessarily teach the "real-time" notification to the user of the portable computing device regarding a "remedial action" to be taken by the user for neutralizing the detected malware, per se). **Rieschick**, see the rejection of Claim 1 above. **Gleichauf**, see the rejection of Claim 1 above) **and**

(ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of service provided to the portable computing device (**Gupta**, does not teach this limitation. **Rieschick**, see the rejection of Claim 1 above, wherein Rieschick teaches that the "user must perform the remedial action or risk deactivation of service provided to the portable computing device", based on the "notification regarding the detected malware event" (but Rieschick does not expressly teach that the "notification" further "specifies a timeframe within which the user must perform the remedial action", which if exceeded actually causes this "deactivation of service provided to the portable computing device"). However, **Gleichauf**, see the rejection of Claim 1 above, wherein Gleichauf does indeed teach specifying a "timeframe" within which the user must perform the remedial action or "risk deactivation of service provided to the portable computing device", and wherein including such a time limit in a malware notification message itself is considered to be obvious over the combination with the malware notification messages of Gupta and/or Rieschick).

See the rejection of Claim 1 for the obviousness motivation for combining the cited prior art references in this manner (i.e., to give the user a predefined amount of time, or “grace period”, for performing the required “remedial actions” for neutralizing the malware, before deactivating network service provided to the mobile device upon expiration of this timeframe).

Regarding Claim 2:

Gupta as modified by Rieschick teaches ...**wherein said detecting a malware event comprises observing activity of the portable computing device that is indicative of malware resident on the portable computing device** (Gupta, see the previously cited excerpts from paragraphs [0019, 0028-0029, 0033-0034, 0041-0042, 0054, 0056-0057], which were not contested by Applicant in the “Reply”.

Rieschick, “detecting and preventing malware from within a mobile data network...detect both known and yet-to-be identified security threats by performing...observed behavior detection methods...monitor network traffic for suspicious content or activities to detect malware and block suspicious data flows from within the network,” paragraph [0027]; “malware system detection component configured to recognize malware based upon patterns within the network traffic and transactions,” paragraph [0028]; “detect transmissions of known and unknown malware in real time as the network patterns emerge...machine learning mechanisms to enable the malware protection system to learn about malware-generated transmissions and recognize malware patterns as they develop...include tracking or correlating network activity levels of recognized threats as well as details of suspicious activities not yet recognized as threatening...store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway),” paragraph [0029]; “detect spam by recognizing network traffic with certain characteristics, which may include destination information, protocols, and/or payload content...detect denial of service attacks by recognizing rapid increases in traffic addressed to a single or related destination from multiple

sources,” paragraph [0031]; “identified security risks...irregular usage patterns,” paragraph [0047]; “policy management system...use the parameters to perform...observed behavior detection methods to determine if the data flow carries malicious content or is otherwise a security risk,” paragraph [0055]; “the policy management system may generate policy rules...based on various factors...subscriber’s usage history...and push the generated rules to the gateway/PCEF,” paragraph [0059]; “the policy management system may compare the IP address information with a list of known offender IP addresses to determine if the IP data flow originates from, or is destined for, a mobile device that is compromised (e.g., infected with malware, a virus, etc.) or blacklisted (e.g., known to intentionally engage in malicious activities),” paragraph [0061]; “the policy management system may generate rules to...perform additional operations (e.g., observed behavior detection methods) to determine if the data flow carries content (e.g., malware) that poses a security risk to a wireless device, network server, or both,” paragraph [0063], similarly see paragraphs [0064-0069] regarding “observed behavior detection methods”).

Regarding Claims 3-4 and 29:

Gupta as modified by Rieschick teaches (Claims 3-4) **...wherein said detecting a malware event comprises detecting malicious content within the data stream...comprises performing pattern matching of content within the data stream with one or more of signatures or rules.** (Claim 29) **...wherein the malware detection module further applies one or more rules to content within the data stream or matches the content with one or more signatures (Gupta,** see the previously cited excerpts from paragraphs [0019, 0028-0029, 0032-0033, 0041-0042, 0054-0055, 0065], which were not contested by Applicant in the “Reply”. **Rieschick,** *“performing a detection method to determine if the data flow carries malicious content,”* paragraph [0006]; *“Pattern matching detection methods...to determine if the data flow carries content that is a security risk...by*

comparing identified binary-file characteristic information with a binary-file characteristic of a known malware type to determine if the data flow carries content having binary-file characteristics of known malware," paragraph [0008]; "detecting and preventing malware from within a mobile data network...detect both known and yet-to-be identified security threats by performing pattern matching...methods...monitor network traffic for suspicious content or activities to detect malware and block suspicious data flows from within the network," paragraph [0027]; "malware system detection component configured to recognize malware based upon patterns within the network traffic and transactions," paragraph [0028]; "detect transmissions of known and unknown malware in real time as the network patterns emerge...machine learning mechanisms to enable the malware protection system to learn about malware-generated transmissions and recognize malware patterns as they develop...store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway)," paragraph [0029]; "detect spam by recognizing network traffic with certain characteristics, which may include destination information, protocols, and/or payload content," paragraph [0031]; "a set of intelligent policy rules...to control the bandwidth, the quality of service and the characteristics of the data, services and flows being communicated between the service network 36 and end users," paragraph [0035]; "The gateway/PCEF 14 may contain a deep packet inspection (DPI) component...configured to obtain additional application-level information about a particular IP data flow," paragraph [0038]; "The policy rules may further govern whether specific IP data flows should be "blocked", "allowed" or "allowed with constraints", based on current and potential security risks/malware threats," paragraph [0046]; also see paragraphs [0047, 0054-0055, 0057-0060, 0069] for additional specific implementation details regarding applying various "pattern matching" techniques, which may be "rule-based" and/or "signature"-based, for detecting "malicious content within the data stream").

Regarding Claims 5 and 22:

Gupta as modified by Rieschick and Gleichauf teaches (Claim 5) **...wherein the malware event is associated with one or more of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content, a security breach and a security violating application.** (Claim 22) **...wherein the detected malware event comprises existence of malicious content within the data stream in a form of one or a combination of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content and a security breach or a security violation** (Gupta, see the previously cited excerpts from paragraphs [0028-0029, 0032, 0034, 0041-0042, 0054, 0057], which were not contested by Applicant in the "Reply". Rieschick, "malicious content," paragraph [0006]; "security risk...known malware type...spam-sending Internet bot," paragraph [0008]; "malware such as computer viruses, computer worms, Trojan horses, bots, spyware, adware, etc.," paragraph [0024]; "malicious software (malware)...attacks (e.g., denial of service attacks) and inconveniences (e.g., spam) caused by malware...security threats...suspicious content or activities...suspicious data flows," paragraph [0027]; "detect spam by recognizing network traffic with certain characteristics...payload content...detect denial of service attacks by recognizing rapid increases in traffic addressed to a single or related destination from multiple sources," paragraph [0031]; "known security risks...emerging security/malware threats," paragraph [0042]; "identified security risks (e.g., known virus, irregular usage patterns, etc.)," paragraph [0047]; "the policy management system may use the received parameters to determine if the data flows carry content (e.g., malware) that poses a security risk to network and/or wireless devices," paragraph [0055]; "known malware types (e.g., bots, viruses, worms, Trojan Horses, etc.)," paragraph [0058], etc. Gleichauf, also teaches that the detected "malware event" may be associated with a "virus", a "worm", "spam",

“malicious content”, an “unauthorized application”, a “security policy violation”, etc.).

Regarding Claims 17 and 30:

Gupta as modified by Rieschick teaches (Claim 17) **...logging, by the malware detection gateway, information regarding the malware event.** (Claim 30) **...a malware information log generation module, which when executed by the one or more processors, logs information regarding the detected malware event** (Gupta, see the previously cited excerpts from paragraphs [0019, 0028-0030, 0032, 0041-0042, 0054-0055, 0057, 0059], which were not contested by Applicant in the “Reply”. Rieschick, “*machine learning capabilities include tracking or correlating network activity levels of recognized threats as well as details of suspicious activities not yet recognized as threatening...store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway) and prevention information (e.g., countermeasures that proved effective in responding to a malware event), which may be used by the malware protection system for the detection and prevention of future malware events,*” paragraph [0029]; “*The user repository 122 may store...user-specific information, such as details of a user’s subscription to malware prevention services and historical details of a user’s exposure to specific malware threats...The policy management system 116 may use the information stored by the user repository 122...to identify potential security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference,*” paragraph [0047]; also see paragraphs [0050-0052, 0055] generally; “*the policy management system may perform quarantining operations by storing details of IP data flows, aggregated details of the IP data flows, or sequestering the actual content of the IP data flows, that were allowed, constrained, or blocked. The policy management system may store source information, destination information and time information for each IP data flow that is constrained...may track the number of IP data flows containing infected binaries within a predetermined time period (e.g., within the last month) and store the*

number value in a memory...may also store emails deemed to be spam," paragraph [0073]).

Regarding Claims 13-14 and 26-27:

Gupta teaches or otherwise suggests (Claim 13) **...wherein the malware indicating message comprises a Diameter message.** (Claim 26) **...wherein the malware-indicating message module queries the user lookup module by sending the user lookup module a Diameter message** (Gupta, paragraphs [0038, 0041-0042] teach sending/receiving messages using the "Diameter" networking protocol, specifically).

Gupta teaches or otherwise suggests (Claim 14) **...wherein the malware indicating message comprises a Remote Authentication Dial In User Service (RADIUS) message.** (Claim 27) **...wherein the malware-indicating message module queries the user lookup module by sending the user lookup module a Remote Authentication Dial In User Service (RADIUS) message** (Gupta, paragraphs [0038, 0041-0042] disclose sending/receiving messages using the "Remote Authentication Dial In User Service (RADIUS)" networking protocol, specifically).

Regarding Claims 6 and 19:

Gupta as modified by Rieschick teaches (Claim 6) **...wherein the malware indicating message further comprises one or more of a time at which the malware event was detected, a type of the malware, a severity of the malware, a security policy violated, a type of security breach, details of the security breach, and properties of the malware.** (Claim 19) **...wherein the information relating to the detected malicious content comprises one or a combination of a time of detection, a type of malware, severity of the malware, a security policy violated, a type of security breach, details of the security breach and properties of the malware** (Gupta, see the previously cited excerpts from

paragraphs [0032-0034, 0041-0042, 0054-0058, 0065, 0067], which were not contested by Applicant in the "Reply". **Rieschick**, *"the gateway/PCEF may examine the data flows and/or the network traffic, identify key characteristics of the data flows and/or network traffic, generate parameters based on the key characteristics and send the generated parameters to a policy management system for analysis...may receive one or more policy rules from the policy management system," paragraph [0054]; "policy management system...receiving parameters from a gateway/PCEF and generating/selecting rules...use the received parameters to determine if the data flows carry content (e.g., malware) that poses a security risk to network and/or wireless devices...determine if the data flow carries malicious content or is otherwise a security risk...generate/select policy rules based on determining the data flows carry content that poses a "known risk," a "potential risk," or "no risk"...send the generate/selected policy rules to the gateway/PCEF for enforcement," paragraph [0055]; "the policy management system may receive parameters identifying certain characteristics of the IP data flows and/or network traffic...examine the parameters to identify/extract information that may be used to determine if the data flow carries content that poses an unacceptable security risk to a wireless device, the network, or both...extract binary-file characteristic information, uniform resource locator (URL) information...IP address information and/or simple mail transfer protocol (SMTP) information...from the received parameters," paragraph [0057]; "the policy management system may compare the extracted binary-file characteristic information with binary-file characteristics of known malware types (e.g., bots, viruses, worms, Trojan Horses, etc.) to determine if the data flow carries content having binary-file characteristics of known malware (e.g., bots viruses, worms, Trojan Horses, etc). If the policy management system determines that the data flow carries content that has binary-file characteristics in common with known malware...generate restrictive policy rules (e.g., "block content," "allow with constraints," etc.) based on the severity of the risk and push the generated rules to the gateway/PCEF...instruct the gateway/PCE to block the*

IP data flow upon determining that an IP data flow carries content having binary-file characteristics of known malware threats (e.g., viruses, Trojan Horses, etc.),” paragraph [0058]; *“the policy management system may compare extracted URL information against a list of URLs known to be under attack (e.g., denial-of-service attack, etc.) to determine if the destination of data flow content is a server under attack. If the policy management system determines that the data flow carries or is likely to carry content destined for a server under attack...generate policy rules (e.g., “block content,” “allow with constraints,” etc.) based on various factors (e.g., severity of the risk, subscriber’s usage history, subscription level, likelihood request is genuine, etc.) and push the generated rules to the gateway/PCEF,”* paragraph [0059]; also see paragraph [0060] generally for another embodiment; *“the policy management system may perform detection methods (e.g., pattern matching, observed behavior, etc.) and generate restrictive policy rules based on the type of malware detected...content having binary-file characteristics of known malware threats (e.g., viruses, Trojan Horses, etc.)...part of a denial of service attack...originates from a spam bot, etc.,”* paragraph [0069]; *“the constraints imposed by the policy management system may be proportional to a malware threat or threat-level as determined by the malware protection system or specified by an operator...determining a malware threat-level within malware protection system...the constraints imposed by the policy management system may become progressively more restrictive or constrained, in real-time, as a malware threat-level rises as determined by malware protection system,”* paragraph [0071]; also see paragraph [0073] generally; *“malware threat model...defined in terms of multiple independent factors, such as the probability of infection, the type of infection, the severity of the threat posed by the infection, and the difficulty associated with removing the infection. These factors may be weighted and combined to produce an overall threat level,”* paragraph [0075]).

Regarding Claims 11 and 23:

Gupta as modified by Rieschick teaches (Claim 11) **...wherein the lookup device includes or forms part of a Policy Control and Resource Function (PCRF) of the mobile service provider network.** (Claim 23) **...wherein the lookup table forms part of a Policy Control and Resource Function (PCRF) of the mobile service provider network** (Gupta, see the previously cited excerpts from paragraphs [0032, 0035, 0038-0039, 0041, 0044, 0046-0047, 0050-0051, 0061], which were not contested by Applicant in the "Reply". Rieschick, see paragraphs [0035, 0039, 0043-0048] regarding a *"policy and charging enforcement function (PCEF) 114"/"PGW 32"* (i.e., the claimed "malware detection gateway device") communicating with a *"policy management system 116"/"policy control rules function (PCRF) 34"* (i.e., the claimed "lookup device" including a "lookup table")).

Regarding Claims 12 and 24:

Gupta as modified by Rieschick teaches (Claim 12) **...wherein the lookup device includes or forms part of a Mobile Device Management (MDM) function of the mobile service provider network.** (Claim 24) **...wherein the lookup table forms part of a Mobile Device Management (MDM) function of the mobile service provider network** (Gupta, see the previously cited excerpts from paragraphs [0013, 0018, 0027, 0032, 0042-0043, 0045, 0056-0057, 0059, 0066-0067, 0079], which were not contested by Applicant in the "Reply". Rieschick, *"a mobility management entity (MME) 26...may request user and subscription information from a home subscriber server (HSS) 42, perform various administrative tasks (e.g., user authentication, enforcement of roaming restrictions, etc.), select a SGW 28 and send administrative and/or authorization information to the SGSN 24,"* paragraph [0034]).

Regarding Claim 25:

Gupta as modified by Rieschick teaches **...wherein the lookup table is stored in a database operatively coupled with the mobile service provider network**

(Gupta, see the previously cited excerpts from paragraphs [0012, 0051-0052], which were not contested by Applicant in the “Reply”. Rieschick, see Fig. 3A; “*The malware protection system 126 may also include a local malware prevention memory or database 127 for each policy management system 116. Likewise, the policy management system 116 may include a local policy management memory...which may be populated by the policy management system 116, the malware protection system 126, or both...the malware protection system 126 may push data to the policy management memory of the policy management system 116...the policy management system 116 may periodically request information from the malware protection system 126 and populate the policy management memory with the received information,*” paragraph [0043]; “*control network 150 (e.g., PCC network)...may include...a user repository 122...may include a subscriber profile repository (SPR),*” paragraph [0044]; “*The user repository 122 may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific information, such as details of a user’s subscription to malware prevention services and historical details of a user’s exposure to specific malware threats,*” paragraph [0047]; also see paragraphs [0039, 0041, 0055, 0074] regarding a “user repository 122” generally).

Regarding Claims 15 and 20:

Gupta as modified by Rieschick teaches (Claim 15) **...responsive to receipt of the malware indicating message, identifying the user by the lookup device based on the IP address.** (Claim 20) **...wherein the unique identifier comprises an Internet Protocol (IP) address associated with the portable computing device** (Gupta, see the previously cited excerpts from paragraphs [0011-0012, 0016, 0025-0026, 0029-0030, 0032-0033, 0039, 0041-0042, 0051-0052, 0055-0056, 0065-0067], which were not contested by Applicant in the “Reply”. Rieschick, “*may map specific malware threats identified to users of the network. Malware threats may be identified using any suitable mechanism, including the use of IP*

addresses,” paragraph [0029]; “the user repository 122 may include a subscriber profile repository (SPR),” paragraph [0044]; “The user repository 122 may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific information,” paragraph [0047]; “the policy management system may compare the IP address information with a list of known offender IP addresses to determine if the IP data flow originates from, or is destined for, a mobile device that is compromised (e.g., infected with malware, a virus, etc.) or black-listed (e.g., known to intentionally engage in malicious activities). If the policy management system determines that the IP address information is associated with an IP address in the list of known offender IP addresses...generate policy rules that block or restrict the data flow and push the generated rules to the gateway/PCEF for enforcement...generate an “allow with constraints” rule upon determining that the IP data flow carries content originating from, or destined for, a mobile device that is compromised or black-listed,” paragraph [0061]].

Regarding Claims 16 and 28:

Gupta as modified by Rieschick teaches (Claim 16) **...extracting information relating to the user, wherein the information comprises calling patterns, message patterns, application usage patterns, types of content accessed by the portable computing device and user attributes.** (Claim 28) **...wherein the user lookup module further extracts information relating to the user, wherein the information comprises calling patterns, message patterns, application usage patterns, types of content accessed by the portable computing device and user attributes** (Gupta, see the previously cited excerpts from paragraphs [0011, 0019, 0033-0034, 0042, 0056-0058, 0066-0067], which were not contested by Applicant in the “Reply”. Rieschick, “store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway) and prevention information (e.g., countermeasures that proved effective in responding to a malware event), which may be used by the malware protection

Art Unit: 2496

system for detection and prevention of future malware events,” paragraph [0029]; “the user repository 122 may include a subscriber profile repository (SPR),” paragraph [0044]; “The user repository 122 may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific information, such as details of a user’s subscription to malware prevention services and historical details of a user’s exposure to specific malware threats...The policy management system 116 may use the information stored by the user repository 122...to identify potential security risks/malware threats and user preferences for responding to identified security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference. The policy management system 116 may make the rule decisions on a per-subscriber, per-session and/or per service basis. For example, the policy management system 116 may use subscriber information (e.g., subscriber’s city of residence), the current usage parameters (e.g., day of week, time of day, peak hours, etc.) and the subscriber’s service level (e.g., Gold, Bronze, etc.) in conjunction with identified security risks (e.g., known virus, irregular usage patterns, etc.) and user preferences to generate and/or select one or more rules or rule groups, which are pushed to the gateway/PCEF 114 for enforcement,” paragraph [0047]; also see paragraphs [0050-0052, 0055, 0064-0067, 0070, 0072] generally).

Regarding Claims 7-9:

Gupta as modified by Rieschick teaches or otherwise suggests (Claim 7)

...sending, by the malware detection gateway device, the malware reporting/notification message to the user responsive to receiving user details from the lookup device (Gupta, see the previously cited excerpts from paragraphs [0032-0035, 0042, 0045, 0056, 0059], which were not contested by Applicant in the "Reply". **Rieschick,** *“store user-specific malware detection (e.g., patterns in network traffic that occurred while a malware event was underway) and prevention information (e.g., countermeasures that proved effective in responding*

to a malware event), which may be used by the malware protection system for detection and prevention of future malware events...map specific malware threats identified to users of the network. Malware threats may be identified using any suitable mechanism, including the use of IP addresses,” paragraph [0029]; “The notification server 128 may be configured to...send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems...the notification server 128 may send messages to a client application running on the mobile devices 102 (e.g., via the Internet 107, access gateway 110, etc.),” paragraph [0039]; “the user repository 122 may include a subscriber profile repository (SPR),” paragraph [0044]; “The user repository 122 may store subscriber information (e.g., customer IDs, preferences, subscription levels, etc.) and user-specific information, such as details of a user’s subscription to malware prevention services and historical details of a user’s exposure to specific malware threats...The policy management system 116 may use the information stored by the user repository 122...to identify potential security risks/malware threats and user preferences for responding to identified security risks/malware threats and make rule decisions based on a combination of the risk/threat and user preference. The policy management system 116 may make the rule decisions on a per-subscriber, per-session and/or per service basis. For example, the policy management system 116 may use subscriber information (e.g., subscriber’s city of residence), the current usage parameters (e.g., day of week, time of day, peak hours, etc.) and the subscriber’s service level (e.g., Gold, Bronze, etc.) in conjunction with identified security risks (e.g., known virus, irregular usage patterns, etc.) and user preferences to generate and/or select one or more rules or rule groups, which are pushed to the gateway/PCEF 114 for enforcement,” paragraph [0047]; “the gateway/PCEF upon the detection of low-risk malware is to send an alert message to the wireless device,” paragraph [0072]; also see paragraph [0077] generally).

Gupta as modified by Rieschick teaches or otherwise suggests (Claim 8)

...triggering the malware reporting/notification message to be sent by the lookup device responsive to the malware indicating message (Gupta, see the previously cited excerpts from paragraphs [0032-0033, 0042, 0056, 0059], which were not contested by Applicant in the "Reply". **Rieschick**, *"The notification server 128 may be configured to receive requests from the policy management system 116 (e.g., PCRF) and send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems,"* paragraph [0039]; *"user preference parameters may be generated from information from a subscriber account in the user repository, by interacting with the user (e.g., via SMS messages sent through the notification server 126, etc.)...a wireless device user may upload user preference parameters to the user repository that instructs the policy management system to send an alert to the user's wireless device warning of potential risks,"* paragraph [0074]; also see paragraph [0077] generally).

Gupta as modified by Rieschick teaches or otherwise suggests (Claim 9)

...triggering the malware reporting/notification message to be sent by a network operator of the mobile service provider network responsive to the malware indicating message (Gupta, see the previously cited excerpts from paragraphs [0033, 0035, 0042, 0045, 0056, 0059], which were not contested by Applicant in the "Reply". **Rieschick**, *"alert wireless device users of detected malware...alert telecommunications network operators of detected malware so they can take corrective actions and/or warn targets of an attack,"* paragraphs [0029]; *"may send detection and prevention information to telecommunications network operators, wireless devices and/or malware systems in real time,"* paragraph [0032]; *"telecommunications network operators and their customers may customize responses to malware events, which may be implemented in real time, consistent*

with the type of threat and how the network operator and/or customer prefers to respond,” paragraph [0070]).

Examiner Note – Claims 7-9 are all obvious variations regarding the particular manner in which the “malware reporting/notification message” may actually be sent and delivered to the user of the portable computing device: (1) by a “malware detection gateway device” (i.e., responsive to receiving “user details” from the “lookup device”, such as an email address or mobile phone number that is mapped to the user device’s IP address), (2) by a “lookup device” directly (i.e., again, responsive to determining “user details” such as an email address or mobile phone number based on the “unique identifier”/“IP address” included in the “malware indicating message”), or similarly (3) by a “network operator” of the mobile service provider network. These claims do not clearly indicate whether or not this malware notification message delivery aspect must necessarily involve three separate and physically distinct hardware computing devices in each respective alternative embodiment. The broad interpretation under BRI is further supported by the fact that Applicant's specification discloses that this functionality may be implemented via a single computing device or may be distributed, and because Claim 18 describes the functionality of these respective devices in terms of various software “modules”. For example, in Gupta the “network threat behavior and analysis engine 6” comprises both “deep netflow inspection engine 7” (i.e., “malware detection gateway device”) as well as “correlation module 36” (i.e., “lookup device”, and is coupled via “reporting module 44” to “management console 40” (i.e., which is accessed by authorized “network operators” or other administrative users of the mobile service provider). Thus, it would be a straightforward, trivial, and obvious design implementation that the user may be notified of a detected malware event associated with their portable computing device automatically by “network threat behavior and analysis engine 6” (i.e., via the interaction of

“deep netflow inspection engine 7”, “correlation module 36”, and “reporting module 44”) and/or manually by a network “operator” that is authorized to access “management console 40” and contact the user. Similarly, Rieschick teaches or otherwise suggests in an obvious manner that malware notification messages may be delivered to a user of a portable computing device (i.e., via email, SMS texts, etc.) by any of the “gateway/PCEF” and/or “policy management system”, the “notification server”, and/or “telecommunications network operators” in different embodiments and depending on user preferences for such malware-related messaging.

Regarding Claims 10 and 21:

Gupta as modified by Rieschick teaches (Claim 10) **...wherein the malware reporting/notification message comprises one or more of sending the user one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, and a Multimedia Messaging Service (MMS).** (Claim 21) **...wherein the malware reporting module is further configured to send a notification to the user in a form of one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, and a Multimedia Messaging Service (MMS) (Gupta**, see the previously cited excerpts from paragraphs [0018, 0025, 0032-0033, 0056, 0059], which were not contested by Applicant in the “Reply”. Based on the disclosure in these paragraphs, the “subscriber” (i.e., the “user of a “subscriber device 12”) is notified of a malware report associated with their network traffic via any suitable messaging technique in the disclosed mobile networking environment. The rationale is that, because such portable computing device of the user comprises a mobile phone (such as a smartphone), it is necessarily configured with various well-known communication functionality (e.g., text messages (SMS) and/or multimedia messages (MMS), phone calls, and/or e-mails), wherein any one or more of these functions may be utilized to share the subscriber-specific behavior reports in order

Art Unit: 2496

to educate users about their traffic patterns and any potentially malicious behavior in the network, so that it may then be addressed accordingly. **Rieschick**, *"The notification server 128 may be configured to...send messages to mobile devices 102 using various technologies/mechanisms, such as email, short message service (SMS) texts, instant messaging (IM) systems, interactive voice response (IVR) systems...depending on the user's preferences and/or mobile device type,"* paragraph [0039]; *"interacting with the user (e.g., via SMS messages sent through the notification server 126, etc.)...instructs the policy management system to send an alert to the user's wireless device warning of potential risks,"* paragraph [0074]).

Regarding Claim 31:

Gupta as modified by Rieschick and Gleichauf teaches **...wherein the portable computing device comprises a smartphone, a mobile phone, a Personal Digital Assistant (PDA) or a tablet personal computer** (**Gupta**, *"A mobile phone...A smartphone,"* paragraph [0018]; *"A 'subscriber device'...is intended to refer to a smartphone,"* paragraph [0020]. **Rieschick**, *"the terms 'mobile device,' 'wireless device' and 'user equipment (UE)'...refer to any one of various cellular telephones, smart-phones (e.g., iPhone), personal data assistants (PDAs), palm-top computers...and similar electronic devices,"* paragraph [0022]. **Gleichauf**, *"The user device or computerized device 22...include, but are not limited to, personal computers (e.g., laptop computers)...IP-enabled and cellular telephones, personal digital assistants (PDA's), etc.,"* Col. 8, lines 38-43).

Conclusion

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

Art Unit: 2496

- a. **McNamee et al. (US 2012/0255019)** - teaches a method and system for malware detection, alert generation, subscriber identification, subscriber notification, and malware remediation.
- b. **Kirti et al. (US 2015/0172321)** – see paragraphs [0096, 0101-0103, etc.].

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER RUPRECHT whose telephone number is (571)272-3844. The examiner can normally be reached on 9am-5pm, M-F.

Art Unit: 2496

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jung Kim can be reached on (571)272-3804. 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.

/CHRISTOPHER RUPRECHT/
Examiner, Art Unit 2494

/THEODORE C. PARSONS/
Primary Examiner, AU2494

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc. Inventor: Rainer Baeder App. No.: 14/617,787 Filed: February 9, 2015 For: MOBILE MALWARE DETECTION AND USER NOTIFICATION	Examiner: Ruprecht, Christopher S. Group Art Unit: 2496 Conf. No.: 1008 Docket No.: FORT-012700
---	--

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

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE PATENT TRIAL AND APPEAL BOARD

Sir/Madam:

Applicant (hereafter “**Appellant**”) hereby submits this Brief in support of its appeal from a decision by the Examiner, mailed November 2, 2017, in the above-captioned application.

Appellant respectfully requests consideration of this Appeal by the Patent Trial and Appeal Board (the “**Board**”) for allowance of the above-captioned patent application.

The claims of the above-captioned patent application were finally rejected by the Examiner in a final Office Action mailed November 2, 2017 (the “**Final Office Action**”). On January 2, 2018, the Appellant submitted a Notice of Appeal (via EFS Web) in the above-captioned patent application. Therefore, this is a proper Appeal and Appellant’s Brief in support of this Appeal follows.

TABLE OF CONTENTS

Table of Contents.....	2
Real Party in Interest.....	3
Related Appeals and Interferences.....	4
Status of Claims	5
Status of Amendments	6
Summary of Claimed Subject Matter	7
Grounds of Rejection to Be Reviewed on Appeal	10
Argument	11
Claims Appendix	24
Evidence Appendix	31
Related Proceedings Appendix	32

REAL PARTY IN INTEREST

The real party in interest in this Appeal is Fortinet, Inc., the assignee of record of the above-referenced patent application.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences related to this Appeal.

STATUS OF CLAIMS

Claims 1-31 are currently pending in the above-captioned patent application. In the Final Office Action, the Examiner rejected claims 1-31 under 35 U.S.C. §103 as allegedly being obvious over US Pub. No. 2014/0189861 of Gupta et al. (hereafter “**Gupta**”), in view of US Pub. No. 2012/0233656 of Rieschick et al. (hereafter “**Rieschick**”), and in further view of US Patent No. 9,436,820 of Gleichauf et al. (hereafter “**Gleichauf**”) in further view of US Patent No. 9,378,359 of Qureshi et al. (hereafter “**Qureshi**”) in further view of US Pub. No. 2014/0128020 of Ramprasad et al. (hereafter “**Ramprasad**”).

Claims 1-31 as set forth in the Amendment and Response to Office Action submitted August 22, 2017 (the “**Amendment and Response**”), are the subject of this Appeal. The Claims Appendix below sets forth a copy of the appealed claims.

STATUS OF AMENDMENTS

No amendment was filed subsequent to the Final Office Action. Consequently, claims 1-31 are appealed in the form presented in the Amendment and Response.

SUMMARY OF CLAIMED SUBJECT MATTER

Technological Background

Embodiments of the present invention relate to detection of mobile malware (e.g., viruses, Trojans, worms or spyware that may be used to disrupt the operation of or gather sensitive information from mobile or portable data processing devices, such as smartphones, tablet computers and personal digital assistants (PDAs)). As noted in the Background of the above-captioned patent application, as sensitive and critical data are now more frequently exchanged via mobile devices, such devices are increasingly the target of intruders, attackers and malware developers. The security of mobile devices is weaker than that of desktop and laptop computer systems for several reasons, including, but not limited to, the power consumption required to continuously run mobile security applications, the different nature of the software architecture of mobile devices, limitations associated with mobile device operating systems and the high processing power and large memory requirements needed to perform comprehensive signature matching as a local malware detection methodology. As such, rather than installing anti-virus or intrusion prevention system (IPS) based security tools on the mobile devices, the inventor suggests the use of an improved malware detection and notification methodology for mobile devices that is implemented by a malware detection gateway device located within a network of a mobile service provider.

Independent Claims

Two independent claims (i.e., claims 1 and 18) are pending in the above-captioned patent application that is the subject of this Appeal. Independent claim 1 relates to a method of detecting the existence of mobile malware on a mobile device by performing analysis

of data communicated to or from the mobile device via the mobile service provider's network rather than attempting to perform local malware scanning¹. A malware event is detected by a malware detection gateway device associated with a network of a mobile service provider based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the network². Responsive to detection of the malware event, a malware reporting/notification message is caused to be sent to a user of the portable computing device in real-time, by sending, by the malware detection gateway device, a malware indicating message to a lookup device³. The malware indicating message includes an Internet Protocol (IP) address of the portable computing device⁴. The malware reporting/notification message includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information⁵. The malware reporting/notification message also specifies a timeframe within which the user must perform the remedial action or risk deactivation of wireless service provided to the portable computing device by the mobile service provider⁶.

Independent claim 18 relates to a malware detection system operable within a network of a mobile service provider⁷. The malware detection system includes one or more processors, a communication interface device and one or more internal data storage devices operatively coupled to the one or more processors and storing instructions representing various modules,

¹ See, e.g., Specification at FIG. 1 (gateway devices 116-1 and 116-2), FIGs. 3A-C (malware detection gateway device 302), FIG. 6 and ¶¶ [0003]-[0007], [0035]-[0036], [0055]-[0057] and [0064].

² See, e.g., Specification at FIG. 1 (gateway devices 116-1 and 116-2), FIG. 6 and ¶¶ [0007], [0017] (examples of malware events), [0035]-[0036], [0055]-[0057] and [0065].

³ See, e.g., Specification at FIGs. 3A-C, FIG. 4 (lookup table 408), FIG. 6 and ¶¶ [00020], [00039], [00050]-[00051], [00054] and [00066]-[00067].

⁴ See, e.g., Specification at FIGs. 3A-C, FIG. 4 and ¶¶ [00055] and [00067].

⁵ See, e.g., Specification at FIGs. 3A-C, FIG. 4 and ¶¶ [00048], [00051]-[00052], [00060] and [00067].

⁶ See, e.g., Specification at FIGs. 3A-C, FIG. 4 and ¶¶ [00051]-[00052], [00060] and [00067].

⁷ See, e.g., Specification at FIG. 1 (gateway devices 116-1 and 116-2), FIGs. 3A-C (malware detection gateway device 302), FIG. 6 and ¶¶ [0003]-[0007], [0035]-[0036], [0055]-[0057] and [0064].

including a malware detection module, a user lookup module, a malware-indicating message module and a malware reporting module⁸. The malware detection module detects a malware event associated with a data stream originating from or directed to a portable computing device communicating with a packet data network via the network⁹. The user lookup module identifies a user corresponding to the portable computing device based on a lookup table and a unique identifier associated with the portable computing device¹⁰. The malware-indicating message module queries the user lookup module by providing information relating to the detected malware event and the unique identifier¹¹. Responsive to the detected malware event, the malware reporting module provides a notification to the user in real-time regarding the detected malware event¹². The notification includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information¹³. The notification also specifies a timeframe within which the user must perform the remedial action or risk deactivation of wireless service provided to the portable computing device by the mobile service provider¹⁴.

⁸ See, e.g., Specification at FIG. 2, FIG. 7 and ¶¶ [00027]-[00029], [00044], [00068]-[00077].

⁹ See, e.g., Specification at FIG. 2, FIG. 6 and ¶¶ [0007], [0017] (examples of malware events), [0035]-[0036] [00045]-[00046], [0055]-[0057] and [0065].

¹⁰ See, e.g., Specification at FIG. 2, FIG. 4 (lookup table 408), FIG. 6 and ¶¶ [00049]-[00050] and [00067].

¹¹ See, e.g., Specification at FIG. 2, FIG. 6 and ¶¶ [00048]-[00049] and [00066]-[00067].

¹² See, e.g., Specification at FIG. 2, FIGs. 3A-C, FIG. 6 and ¶¶ [00020], [00039], [00050]-[00051], [00054] and [00067].

¹³ See, e.g., Specification at FIGs. 3A-C, FIG. 4 and ¶¶ [00048], [00051]-[00052], [00060] and [00067].

¹⁴ See, e.g., Specification at FIGs. 3A-C, FIG. 4 and ¶¶ [00051]-[00052], [00060] and [00067].

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

- A. Did the Examiner fail to make out a **prima facie** case of obviousness as a result of including non-analogous art as part of the proposed combination of prior art?

- B. Did the Examiner improperly reject claims 1-31 under 35 U.S.C. §103 by attributing capabilities and functionality to one or more of the relied upon references that are clearly unsupported by and outside of the scope and contemplation of their respective disclosures?

ARGUMENT

- A. The Examiner failed to make out a **prima facie** case of obviousness as a result of including three non-analogous prior art references as part of the proposed five-prior-art-reference combination.

Claims 1-31

In the Final Office Action, the Examiner proposes combining the teachings from a hodgepodge of five prior art references from differing fields, including **wireless service usage tracking, Network Access Control (NAC) and malware detection in the context of mobile data network environments**. The undersigned respectfully asserts the Examiner has failed to make out a **prima facie** case of obviousness as a combination of non-analogous art is insufficient to render the claims **prima facie** obvious.

The Federal Circuit has adopted a “two-step test” for determining whether a particular reference is within the appropriate art. First, a determination is made regarding whether the reference at issue is “within the field of the inventor’s endeavor.” Second assuming the reference is outside of that field, it must be determined whether the reference is “reasonably pertinent to the particular **problem** with which the inventor was involved.” See In re Deminiski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986) (emphasis added). As such, a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). See In re Bigio, 381 F.3d at 1325, 72 USPQ2d at 1212.

Overview of the Three Non-Analogous References

While the undersigned acknowledges Gupta and Rieschick are in analogous field (i.e., malware detection within a mobile data network environment based on monitoring of traffic), the undersigned respectfully asserts Gleichauf, Qureshi and Ramprasad are in fields different from that of Gupta, Rieschick and the above-captioned patent application.

Gleichauf relates to the field of Network Access Control (NAC), which those skilled in the art understand to involve evaluation of the **compliance** of a client device attempting to connect to a network **with the policies** of a network **before granting the client device access** to the network or a resource thereof. For example, a client attempting to access a network may be required to implement a particular level of anti-virus protection or have certain operating system patches installed. See, e.g., Gleichauf at col. 2, ll. 46-54 and col. 4, ll. 32-40 (“admitting computerized devices onto a network” based on its security state or “posture”).

Qureshi also relates to the field of NAC. See, e.g., mobile device management systems 126 and secure mobile gateways 128 of Qureshi at FIGs. 1A-E, col. 1, ll. 17-22 (“systems for ... management of devices used for accessing managed resources of an enterprise”) and col. 11, l. 59 – col. 12, l. 9 (mobile device access to enterprise resources may be controlled based on the configuration of the mobile device at issue).

Ramprasad relates to the field of wireless service usage tracking. See, e.g., Ramprasad at ¶¶ [0002] (“metering server and tracking client for wireless services”) and [0014] (need for the ability to track and/or meter wireless services used by subscribers having handsets with an open mobile OS). While the Examiner attempts to shoehorn Ramprasad into the field of “network security” based on ¶¶ [0077], [0087] and [0088] of Ramprasad, the undersigned notes

the software required to be installed on the wireless device 104 is a **tracking client 154** (Client 154 in FIG. 1 of Ramprasad), which is described by Ramprasad as being for the purpose of **tracking the usage of the wireless device 104 and/or for reporting usage information to the metering server 150**. See, e.g., Ramprasad at ¶ [0049]. Nowhere in the portions of Ramprasad relied upon by the Examiner or elsewhere in Ramprasad is there any contemplation that the tracking client 154 relates to network security generally or malware detection within a mobile data network environment more specifically. Notably, the “fraudulent activity” referred to in ¶¶ [0087]-[0088] of Ramprasad relates to tampering with or removal of the tracking client 154 by the mobile subscriber in an attempt to obtain wireless service in excess of that paid for, for example. The undersigned respectfully asserts the Examiner’s statement indicating “[t]his is also directed to network security and **the proper software** that is installed could be the malware software present in the other references used in the rejection” is pure speculation on the Examiner’s part and finds no support in Ramprasad. See Final Office Action at p. 3. Emphasis added. Nowhere in Ramprasad is there any mention of “malware.” The only “proper software” confirmed to be installed in the context of Ramprasad is the **tracking client 154**, which serves no network security purpose, but rather seeks to track wireless usage by the wireless device 104 at issue.

The Field of Endeavor of Independent Claims 1 and 18

The Examiner takes the position that the relevant field is the broad concept of “network security.” The undersigned respectfully disagrees. Techopedia confirms “network security is an **over-arching term** that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or

denial of the network and network resources.” See

<https://www.techopedia.com/definition/24783/network-security>. Emphasis added.

Further evidence of the breadth of the concept of network security is the fact that **the network security industry includes many diverse fields** including, but not limited to, authentication, access policies, wireless security, endpoint security, mobile security, data loss prevention and intrusion prevention. Networks are subject to many types of attacks including, but not limited to, viruses, eavesdropping, data modification, denial-of-service attacks, Domain Name System (DNS) spoofing, man-in-the-middle attacks, Address Resolution Protocol (ARP) poisoning, Virtual Local Area Network (VLAN) hopping, Smurf attack, buffer overflow, heap overflow, format string attack, Structured Query Language (SQL) injection, phishing, cross-site scripting and Cross-Site Request Forgery (CSRF).

Under the Examiner’s over inclusive analogous art analysis, prior art references relating to very different fields associated with the concept of network security (i.e., (i) SQL injection, a code injection technique used to attack databases and (ii) DNS spoofing, an attack that diverts Internet traffic away from legitimate servers and towards fake ones) would be considered analogous and properly combinable despite their very different functions. This is clearly improper. The United States Court of Customs and Patent Appeals (CCPA) found “the similarities and differences in structure and function of the inventions to carry far greater weight [than classification evidence].” In re Ellis, 476 F.2d 1370, 1372, 177 USPQ 526, 527 (CCPA 1973) (The structural similarities and functional overlap between the structural gratings shown by one reference and the shoe scrapers of the type shown by another reference were readily apparent, and therefore the arts to which the reference patents belonged were reasonably pertinent to the art with which appellant’s invention dealt (pedestrian floor gratings).). Applying

In re Ellis to the present circumstances, in which the Examiner attempts to combine teachings from the field of **Network Access Control (NAC)** (i.e., Gleichauf and Qureshi) and teachings from the field of **wireless service usage tracking** (i.e., Ramprasad), both of which involve disparate functionality (as explained above) unrelated to that of (i) independent claim 1, which is directed to a method of **detecting the existence of mobile malware on a mobile device by performing analysis of data communicated to or from the mobile device via the mobile service provider's network**, and (ii) independent claim 18, which is directed to **a malware detection system operable within a network of a mobile service provider**, results in a finding that Gleichauf, Qureshi and Ramprasad are non-analogous to the field of endeavor of claims 1 and 18.

Further evidence of the field of endeavor of the claims is the disclosure of which they are a part. While admittedly the above-captioned patent application notes in various places concerns for the security of the mobile service provider's network, the vast majority of the disclosure is focused on how to perform malware detection and mobile device end-user notification within a mobile data network environment to address the problem of **the difficulties of performing malware scanning on mobile devices** (e.g., smartphones). See, e.g., Specification at FIG. 1 and ¶¶ [0003]-[0006], [00017] and [00034]-[00043]. Similarly, the title of the above-captioned patent application (i.e., "Mobile Malware Detection and User Notification") makes clear the inventor's field of endeavor relates more specifically to a malware detection methodology applicable to mobile devices. As such, the undersigned respectfully submits a more appropriate characterization of the field of endeavor for independent claims 1 and 18 is malware detection within a mobile data network environment based on monitoring of traffic.

The Problem Addressed

The problem addressed by the above-captioned patent application relates to **the difficulties of performing malware scanning on mobile devices** (e.g., smartphones), which may be memory constrained and which may have limited processing capabilities. See, e.g., Specification at ¶¶ [0003] and [0005]. To address this problem, the above-captioned patent application suggests the use of a malware detection gateway device associated with a network of a mobile service provider to detect malicious content within a data stream transmitted to or from a portable computing device communicating with a packet data network via the network. See, e.g., Specification at FIG. 1 and ¶¶ [00018] and [00036].

Since Gleichauf, Qureshi and Ramprasad are in fields different from that of Gupta, Rieschick and the field of endeavor of the claims as shown above, the next step is to determine the **pertinence** of Gleichauf, Qureshi and Ramprasad **to the particular problem** addressed by the above-captioned patent application. Gleichauf's alleged improvement relates to evaluating the "security posture" of a device at the time it attempts to connect to the network rather than evaluating and scanning devices while they are connected to the network according to a scanning schedule. See, e.g., Gleichauf at col. 2, ll. 46-57 and col. 3, ll. 4-9. As such, Gleichauf is not concerned with addressing the difficulties of performing malware scanning on mobile devices, but rather determining whether devices connecting to the network at issue have a configuration state or "security posture" acceptable to the network.

Qureshi's alleged improvement relates to NAC improvements to address the growing trend among businesses to allow employees to use their personally owned mobile devices to access company resources, which is known as "bring your own device" (BYOD) or "bring your own technology" (BYOT). See, e.g., Qureshi at col. 1, ll. 37-44. As such, Qureshi shows no

concern for addressing the difficulties of performing malware scanning on mobile devices, but rather, like Gleichauf, is focused on determining whether devices connecting to the network at issue have a configuration state acceptable to the network. See, e.g., Qureshi at col. 11, l. 59 – col. 12, l. 9 (mobile device access to enterprise resources may be controlled based on the configuration of the mobile device at issue).

Ramprasad's alleged improvement relates to the ability to meter wireless service usage of a wireless device by implementing a hybrid network based metering server and tracking client. See, e.g., Ramprasad at ¶ [0015]. As such, Ramprasad shows no contemplation of the problem addressed by the above-captioned patent application.

In view of the foregoing, it is unreasonable to expect Gleichauf, Qureshi or Ramprasad to have drawn the attention of an inventor attention attempting to solve the problem addressed by the above-captioned patent application and none of Gleichauf, Qureshi and Ramprasad satisfy the Federal Circuit's two-step test. As such, none of Gleichauf, Qureshi and Ramprasad qualifies as being within the appropriate art for combination with Gupta and Rieschick. For at least this reason, the proposed combination of any of Gleichauf, Qureshi and Ramprasad with either of Gupta and Rieschick is improper and cannot properly render the claims **prima facie** obvious. Therefore, the undersigned respectfully requests the Board to reverse the Examiner's obviousness rejections – all of which rely on one or more of Gleichauf, Qureshi and Ramprasad in combination with one or more of Gupta and Rieschick.

B. The Examiner improperly rejected claims 1-31 under 35 U.S.C. §103 by attributing capabilities and functionality to one or more of the relied upon references that are clearly unsupported by and outside of the scope and contemplation of their respective disclosures.

Claims 1-31

In the Final Office Action, the Examiner rejected claims 1-31 under 35 U.S.C. §103 for allegedly being unpatentable over Gupta, in view of Rieschick, in view of Gleichauf, in further view of Qureshi and in further view of Ramprasad. As noted above, the undersigned believes it is improper to combine the non-analogous art references of Gleichauf, Qureshi and Ramprasad with Gupta and Rieschick; however, to the extent the Board determines the Examiner's proposed combination of prior art references is proper (a conclusion with which the undersigned disagrees), the undersigned points out below significant distinctions over the combined teachings of the asserted references.

With respect to independent claim 1, the combination of Gupta, Rieschick, Gleichauf, Qureshi and Ramprasad does not teach or reasonably suggest at least:

- **responsive to said detecting**, causing a malware reporting/notification message to be sent to a user of the portable computing device in real-time ...
- wherein **the malware reporting/notification message ... specifies a timeframe within which the user must perform the remedial action or risk deactivation of wireless service** provided to the portable computing device by the mobile service provider.

With respect to the above-quoted “responsive to said detecting” limitations, the Examiner relies on Gupta for teaching the recited “malware reporting/notification message” is sent to a user responsive to detecting a malware event, citing to ¶¶ [0033], [0035], [0056], [0059]. See Final Office Action at pp. 4 and 9. Notably, however, Gupta does not teach, reasonably suggest or even contemplate a “malware reporting/notification message.” Rather, Gupta simply suggests that “a mobile service provider **may choose to educate subscribers** ... on [sic] their particular behaviors.” See Gupta at ¶ [0033]. Emphasis added. The undersigned notes the Examiner’s reliance on Gupta’s reporting module 44 is misplaced as Gupta simply describes storing network event information and the correlated subscriber device information in an event database and **allowing subscribers visibility into the event database** 46. See Gupta at ¶ [0059]. As such, no “malware reporting/notification message” is contemplated by Gupta – let alone causing one to be sent to a user “responsive to detecting” a malware event. Instead, Gupta merely suggests subscribers might be educated about their behaviors by allowing subscribers to access stored network event information. The Examiner does not rely on any of the other asserted prior art references to teach this limitation and the undersigned finds no such teachings in the other asserted prior art references. For at least this reason, independent claim 1 and its dependent claims, which add further limitations, are thought to be distinguishable over the prior art of record.

Turning now to the above-quoted “wherein” limitations, in the Final Office Action, the Examiner correctly acknowledges Gupta does not teach these limitations. See Final Office Action at pp. 10-11. The Examiner also acknowledges Rieschick does not teach the above-quoted “wherein” limitations. See Final Office Action at p. 19. Furthermore, the Examiner correctly acknowledges Gleichauf does not teach the above-quoted “wherein” limitations. See

Final Office Action at p. 27. However, somehow, the Examiner concludes that because Gleichauf periodically transmits a posture update query message to the posture agent, the “timeframe” associated with the periodic transmission meets the requirement of independent claim 1 that “the malware reporting/notification message ... **specifies a timeframe within which the user must perform the remedial action** or risk deactivation of wireless service” when combined with teachings of Gupta and/or Rieschick.

As an initial matter, the undersigned notes that the Examiner appears to have mischaracterized the teachings of Gupta and Rieschick to support his obviousness conclusions. For example, the Examiner states “[g]iven the teachings of Gupta that the user should be notified of a detected malware event **and information regarding any corresponding remedial actions**, and further coupled with the teachings of Rieschick that **such notifications should be sent to the user ‘in real time’ upon malware detection**, such a person would have considered it to be obvious to have included the time limit of Gleichauf directly into the user malware notification messages of Gupta and/or Rieschick.” First, Gupta does not teach a user should be notified of “information regarding any corresponding remedial actions.” As explained further below, Gupta’s focus is on educating subscribers about their behaviors – no remediation is contemplated. Second, Rieschick does not teach “notifications should be sent to the user in real time” as stated by the Examiner, but rather teaches **detecting** “transmissions of known and unknown malware in real time.” See Rieschick at ¶ [0029]. Later, in the same paragraph, Rieschick states “[v]arious embodiments may alert wireless device users of detected malware,” but there is no suggestion in Rieschick that the detecting and the alerting are connected.

With respect to Gupta, as noted above, it simply suggests that “a mobile service provider **may choose to educate subscribers** ... on [sic] their particular behaviors.” See Gupta at ¶

[0033]. Emphasis added. Meanwhile, the Examiner's reliance on Gupta's reporting module 44 is misplaced as Gupta simply describes storing network event information and the correlated subscriber device information in an event database and allowing subscribers visibility into the event database 46. See Gupta at ¶ [0059]. As such, no "malware reporting/notification message" is contemplated by Gupta. Rather, Gupta simply suggests subscribers might be educated about their behaviors by allowing subscribers to access stored network event information.

With respect to Rieschick, the undersigned acknowledges Rieschick "may alert wireless device users of detected malware" in ¶ [0029]. Notably, however, it is the network that takes remedial action by responsive to detecting a data flow carrying malicious content, generating restrictive policy rules that **instruct a gateway to block the data flow**. As such, it is clear that these remedial actions are not communicated to the end user and are not expected to be implemented by an end user. See Rieschick at ¶¶ [0006] and [0027]. As such, at best, Rieschick teaches completely separate methods of (i) performing gateway implemented remedial actions and (ii) alerting end users regarding detected malware, but there is no connection between the two.

In view of the foregoing, the undersigned respectfully asserts the Examiner's attempt to take the disparate teachings of Gleichauf, Gupta and Rieschick to piece together the above-quoted malware reporting/notification message appears to rely on impermissible hindsight. MPEP § 2142 states that "impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of **the facts gleaned from the prior art**." Emphasis added. In the present case, the Examiner relies on various stated rationales for specifying and permitting a timeframe or grace period that are not supported by the teachings of Gleichauf, Gupta or

Rieschick, but rather appear to be after-the-fact justifications based on Applicant's disclosure in an exercise of impermissible hindsight. Accordingly, for at least these additional reasons, the undersigned requests the Board to reverse the Examiner's obviousness rejection of independent claim 1 and its dependent claims.

Regarding independent claim 18, it includes limitations similar to those discussed above with reference to independent claim 1. Therefore, independent claim 18 and its dependent claims, which add further limitations, are thought to be allowable over the combined teachings of Gupta, Rieschick, Gleichauf, Qureshi and Ramprasad for the reasons presented above in connection with independent claim 1.

As evidenced by the foregoing, the Examiner has incorrectly attributed teachings to at least Gupta and Rieschick that are clearly absent from and not contemplated by their respective disclosures. The Examiner then proceeds to use such attributed teachings to improperly find obviousness under 35 U.S.C. §103. For at least these reasons, the undersigned respectfully requests the Board to reverse the Examiner's rejections of claims 1-31.

CONCLUSION

The Examiner has failed to establish a **prima facie** case of obviousness as a result of including three non-analogous prior art references as part of the proposed five-prior-art-reference combination. Furthermore, to the extent properly combinable, the teachings of various references of the five-prior-art-reference combination have been mischaracterized by the Examiner, thereby undermining the Examiner's conclusions regarding alleged obviousness. For the aforementioned reasons, the Examiner's rejections should be reversed, and claims 1-31 should be allowed.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date March 30, 2018

By: /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 64128
Ph: (720) 458-1830

CLAIMS APPENDIX

1. A method comprising:

detecting, by a malware detection gateway device associated with a network of a mobile service provider, a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the network; and

responsive to said detecting, causing a malware reporting/notification message to be sent to a user of the portable computing device in real-time, by sending, by the malware detection gateway device, a malware indicating message to a lookup device, wherein the malware indicating message comprises an Internet Protocol (IP) address of the portable computing device, wherein the malware reporting/notification message (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information and (ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of wireless service provided to the portable computing device by the mobile service provider.
2. The method of claim 1, wherein said detecting a malware event comprises observing activity of the portable computing device that is indicative of malware resident on the portable computing device.

3. The method of claim 1, wherein said detecting a malware event comprises detecting malicious content within the data stream.
4. The method of claim 3, wherein said detecting malicious content comprises performing pattern matching of content within the data stream with one or more of signatures or rules.
5. The method of claim 1, wherein the malware event is associated with one or more of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content, a security breach and a security violating application.
6. The method of claim 1, wherein the malware indicating message further comprises one or more of a time at which the malware event was detected, a type of the malware, a severity of the malware, a security policy violated, a type of security breach, details of the security breach, and properties of the malware.
7. The method of claim 1, wherein said causing a malware reporting/notification message to be sent to a user of the portable computing device comprises sending, by the malware detection gateway device, the malware reporting/notification message to the user responsive to receiving user details from the lookup device.
8. The method of claim 1, wherein said causing a malware reporting/notification message to be sent to a user of the portable computing device comprises triggering the malware

reporting/notification message to be sent by the lookup device responsive to the malware indicating message.

9. The method of claim 1, wherein said causing a malware reporting/notification message to be sent to a user of the portable computing device comprises triggering the malware reporting/notification message to be sent by a network operator of the network responsive to the malware indicating message.
10. The method of claim 1, wherein the malware reporting/notification message comprises one or more of sending the user one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, and a Multimedia Messaging Service (MMS) message.
11. The method of claim 1, wherein the lookup device includes or forms part of a Policy Control and Resource Function (PCRF) of the network.
12. The method of claim 1, wherein the lookup device includes or forms part of a Mobile Device Management (MDM) function of the-network.
13. The method of claim 1, wherein the malware indicating message comprises a Diameter message.

14. The method of claim 1, wherein the malware indicating message comprises a Remote Authentication Dial In User Service (RADIUS) message.
15. The method of claim 1, further comprising, responsive to receipt of the malware indicating message, identifying the user by the lookup device based on the IP address.
16. The method of claim 14, further comprising extracting information relating to the user, wherein the information comprises calling patterns, message patterns, application usage patterns, types of content accessed by the portable computing device and user attributes.
17. The method of claim 1, further comprising logging, by the malware detection gateway, information regarding the malware event.
18. A malware detection system operable within a network of a mobile service provider comprising:
 - one or more processors;
 - a communication interface device; and
 - one or more internal data storage devices operatively coupled to the one or more processors and storing instructions representing:
 - a malware detection module, which when executed by the one or more processors, detects a malware event associated with a data stream originating from or directed to a portable computing device communicating with a packet data network via the network;

a user lookup module, which when executed by the one or more processors, identifies a user corresponding to the portable computing device based on a lookup table and a unique identifier associated with the portable computing device;

a malware-indicating message module, which when executed by the one or more processors, queries the user lookup module by providing information relating to the detected malware event and the unique identifier; and

a malware reporting module, which when executed by the one or more processors, provides, responsive to the detected malware event, a notification to the user in real-time regarding the detected malware event, wherein the notification (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information and (ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of wireless service provided to the portable computing device by the mobile service provider.

19. The system of claim 18, wherein the information relating to the detected malicious content comprises one or a combination of a time of detection, a type of malware, severity of the malware, a security policy violated, a type of security breach, details of the security breach and properties of the malware.
20. The system of claim 18, wherein the unique identifier comprises an Internet Protocol (IP) address associated with the portable computing device.

21. The system of claim 18, wherein the malware reporting module is further configured to send a notification to the user in a form of one or more of a Short Message Service (SMS) message, a telephone call, an electronic mail (email) message, and a Multimedia Messaging Service (MMS) message.
22. The system of claim 18, wherein the detected malware event comprises existence of malicious content within the data stream in a form of one or a combination of a virus, a trojan, an exploit, an attack, spyware, an unexpected data stream, blocked content and a security breach or a security violation.
23. The system of claim 18, wherein the lookup table forms part of a Policy Control and Resource Function (PCRF) of the network.
24. The system of claim 18, wherein the lookup table forms part of a Mobile Device Management (MDM) function of the network.
25. The system of claim 18, wherein the lookup table is stored in a database operatively coupled with the network.
26. The system of claim 18, wherein the malware-indicating message module queries the user lookup module by sending the user lookup module a Diameter message.

27. The system of claim 18, wherein the malware-indicating message module queries the user lookup module by sending the user lookup module a Remote Authentication Dial In User Service (RADIUS) message.
28. The system of claim 18, wherein the user lookup module further extracts information relating to the user, wherein the information comprises calling patterns, message patterns, application usage patterns, types of content accessed by the portable computing device and user attributes.
29. The system of claim 18, wherein the malware detection module further applies one or more rules to content within the data stream or matches the content with one or more signatures.
30. The system of claim 18, further comprising a malware information log generation module, which when executed by the one or more processors, logs information regarding the detected malware event.
31. The system of claim 18, wherein the portable computing device comprises a smartphone, a mobile phone, a Personal Digital Assistant (PDA) or a tablet personal computer.

EVIDENCE APPENDIX

NONE.

RELATED PROCEEDINGS APPENDIX

NONE.

Electronic Acknowledgement Receipt	
EFS ID:	32214119
Application Number:	14617787
International Application Number:	
Confirmation Number:	1008
Title of Invention:	MOBILE MALWARE DETECTION AND USER NOTIFICATION
First Named Inventor/Applicant Name:	Rainer Baeder
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012700
Receipt Date:	30-MAR-2018
Filing Date:	09-FEB-2015
Time Stamp:	20:41:39
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	Appeal Brief Filed	Appeal_Brief.pdf	195457	no	32
			d12626027e02ac1c729c1a97f27b4114272dd812		

Warnings:

Information:	
Total Files Size (in bytes):	195457
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.	



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/617,787	02/09/2015	Rainer Baeder	FORT-012700	1008
64128 7590 08/23/2018 MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP 12640 W. Cedar Drive, Suite 1 LAKEWOOD, CO 80228			EXAMINER ABRISHAMKAR, KAVEH	
			ART UNIT 2494	PAPER NUMBER
			NOTIFICATION DATE 08/23/2018	DELIVERY MODE ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesantis@hdciplaw.com



UNITED STATES PATENT AND TRADEMARK OFFICE

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

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Application Number: 14/617,787
Filing Date: 9 Feb 2015
Appellant(s): Baeder, Rainer,

Michael A. DeSanctis
Reg. No. 39,957
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 30, 2018.

(1) Grounds of Rejection to be Reviewed on Appeal

Every ground of rejection set forth in the Office action dated November 2, 2017 from which the appeal is taken is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(2) Response to Argument

In broad outline, Gupta¹ teaches² inspecting packets to detect network events (e.g., traffic indicative of malicious activity) and sending the user an alert message. While Gupta does not teach putting countermeasure requirements and a time limit into the message, Rieschick and Gleichauf do teach these limitations. Rieschick teaches that the message should identify countermeasures to be taken by the user device. To this, Gleichauf adds that the countermeasures must be taken within a limited time period. Further, Qureshi explicitly teaches putting required time periods into messages to users. Thus, it would have been obvious for the message Gupta sends to the user responsive to the suspect event to be modified to include countermeasure requirements per Rieschick and a time limit per Gleichauf.

A. The Cited Prior Art is Analogous Art

The Appellant argues that three of the prior art references provided are non-analogous art and therefore fail to make out a prima facie case of obviousness.

The Examiner contends that all the prior art references provided, Gleichauf, Qureshi and Ramprasad, are analogous art. It has been held that a prior art reference must either be in the field of

¹ Claims 1-31 (i.e., all claims) stand rejected under 35 USC 103 as being unpatentable over Gupta et al. (US 2014/0189861), in view of Rieschick et al. (US 2012/0233656), and in further view of Gleichauf et al. (US 9,436,820) in further in view of Qureshi et al. (U.S. Patent 9,378,359) in further in view of Ramprasad et al. (U.S. Patent Pub. No. 2014/0128020).

² Detailed citations are provided below, and in the Final Rejection of October 30, 2017.

applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention.

See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). The Examiner will address each prior art references being attacked individually. First, Gleichauf is directed towards a method of controlling access in a network based on determining the real-time security state of the computerized device to minimize the risk of a device transmitting malware (See Gleichauf, Abstract). Gleichauf further collects information on the security posture of the computer device which can include the possible risk of transmitting malware by determining if virus software is up to date (Gleichauf column 3, lines 30-47). Therefore, both Gleichauf and the claimed invention are directed to reducing the possible effect of malware on devices. Second, Qureshi discloses a system that allows users to securely access resources using their mobile devices by controlling mobile device access based on device attributes or behavioral attributes or other conditions (see Qureshi, Abstract). These conditions can include conditions indicative of detecting malware and would prevent the execution of an application as a result (Qureshi column 96, lines 51-60). Therefore, both Qureshi and the claimed invention are directed to reducing the possible effect of malware on devices. Third, Ramprasad discloses a process of tracking usage of a wireless device and also includes reporting the usage of the wireless services (see Ramprasad, Abstract). Ramprasad further discloses that the metering server will reject the wireless device if all required device verifications are not successful, and if the wireless device deletes a tracking client then a report is sent that results in the deactivation of wireless services (Ramprasad paragraph 0077). This is directed towards the same problem of deactivating wireless services if an improper action (e.g. no tracking client installed) has been realized. Therefore, the Examiner respectfully contends that all three prior art references are analogous art.

B. The Prior Art Teaches Sending the Claimed Notification

The Appellant further argues that the Cited Prior Art (CPA) does not disclose "responsive to said detecting, causing a malware reporting/notification message to be sent to a user of a portable computing device in real-time".

The Examiner contends that the CPA does disclose responsive to said detecting, causing a malware reporting/notification message to be sent to a user of a portable computing device in real-time. Gupta discloses receiving subscriber data traffic and inspecting the packets for network events, which can include detecting malware or other unauthorized activity (Gupta: paragraphs 0054-0055). Gupta then creates network event information including the source or destination of the traffic and an identifier of the network event information (Gupta: paragraph 0055). Furthermore, Gupta provides for a reporting module which can provide information based on the event information to the subscriber (user of the mobile device) (Gupta: paragraph 0059). This information is analogous to the claimed malware reporting/notification message as it is based on the network event information and is sent to the user of the device (subscriber). Furthermore, Rieschick discloses generating restrictive policy rules in response to detecting malware in a mobile data network (Rieschick: paragraphs 0006, 0027-0029). Furthermore, Rieschick detects malware in real-time as network patterns emerge (Rieschick: paragraph 0029). In response to detecting the malware, Rieschick discloses alerting the wireless users of the detected malware so that they can take corrective actions (Rieschick: paragraph 0029). Therefore, the Examiner contends that the CPA does disclose that responsive to said detecting, causing a malware reporting/notification message to be sent to a user of a portable computing device in real-time.

C. The Prior Art Teaches Specifying The Claimed Timeframe for Remediation

The Appellant further argues that the CPA does not teach specifying a timeframe within which the user must perform the remedial action.

The Examiner contends that the CPA does teach specifying a timeframe within which the user must perform the remedial action. Gleichauf discloses a procedure wherein a mobile device is granted or denied access to network resources based on a check of proper configuration or timely execution of the anti-virus application from a particular manufacturer (Figure 1, column 22, lines 38-44). This is performed by providing periodic real-time detection of the security posture or security state of the mobile device which minimizes user devices which are not configured with up-to-date anti-virus applications from accessing the network (column 22, lines 50-58). Gleichauf periodically re-executes the sequence based on the expiration of a present time period or a timer (column 19, lines 4-13). Though this time period is not explicitly stated to be provided in a message, in view of Gupta and Rieschick, it would have been obvious to provide this information to a user device. A person of ordinary skill in the art would know that enforcing a Gleichauf time limit, without informing the user of the timeframe in the countermeasure message of Rieschick would lead to unsuccessful remediation and user frustration. Gupta discloses receiving subscriber data traffic and inspecting the packets for network events, which can include detecting malware or other unauthorized activity (Gupta: paragraphs 0054-0055) and then creates network event information including the source or destination of the traffic, and an identifier of the network event information (Gupta: paragraph 0055). Furthermore, Gupta provides for a reporting module which can provide information based on the event information to the subscriber (user of the mobile device) (Gupta: paragraph 0059). This information is analogous to the claimed malware reporting/notification message as it is based on the network event information and is sent to the user of the device (subscriber). This message does not explicitly include the timer information or which remedial actions need to be taken. Rieschick discloses sending a message to users alerting the wireless users of malware and also providing prevention information (countermeasures) to the devices in real time (paragraphs 0029, 0032). Therefore, the combination of Gupta and Rieschick discloses providing countermeasure information in a message to the users. The actual timeframe which the user has to

implement a remediation or countermeasure is not explicitly disclosed in the combination of Gupta and Rieschick. However, Gleichauf discloses a time period which a user has to execute remediation or be denied access to network resources (Gleichauf: column 22, lines 38-47) and that the security posture is periodically re-checked upon the expiration of a timer (Gleichauf: column 19, lines 4-14). Gupta discloses receiving subscriber data traffic and inspecting the packets for network events, which can include detecting malware or other unauthorized activity (Gupta: paragraphs 0054-0055) and then creates network event information including the source or destination of the traffic, and an identifier of the network event information (Gupta: paragraph 0055). Furthermore, Gupta provides for a reporting module which can provide information based on the event information to the subscriber (user of the mobile device) (Gupta: paragraph 0059). This information is analogous to the claimed malware reporting/notification message as it is based on the network event information and is sent to the user of the device (subscriber). The combination of Gupta and Rieschick with Gleichauf renders obvious the claimed notification message with the timeframe (Gleichauf requires that the remediation or countermeasure is performed before being denied access to network resources). The motivation for this combination would include alerting the users to pertinent information about the security issues to ensure the subscriber has sufficient information for addressing these issues, including how long the user has to perform the fix before access to the network will be denied.

Furthermore, Qureshi discloses that a remedial action can cause an agent to terminate or prevent the mobile device's connection to the unsecured network (column 62, lines 22-30) and provides a message to the user instructing the user to terminate the connection (remedial action) within a **specified** time period (column 62, lines 30-44) and/or providing other instructions in case the connection is not terminated to the agent via a message (column 62, lines 40-52). Hence, Qureshi discloses that a time period is specified in a message that is sent to a user and agent on the user device to perform a remedial action. Therefore, the Examiner contends that the combination of cited prior art renders

obvious the feature specifying a timeframe within which the user must perform the remedial action in the context of the claim as a whole.

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

Respectfully submitted,

/KAVEH ABRISHAMKAR/
Primary Examiner, Art Unit 2494

Conferees:

/THEODORE C PARSONS/
Primary Examiner, Art Unit 2494

/JUNG W KIM/
Supervisory Patent Examiner, Art Unit 2494

Requirement to pay appeal forwarding fee. In order to avoid dismissal of the instant appeal in any application or ex parte reexamination proceeding, 37 CFR 41.45 requires payment of an appeal forwarding fee within the time permitted by 37 CFR 41.45(a), unless appellant had timely paid the fee for filing a brief required by 37 CFR 41.20(b) in effect on March 18, 2013.

Electronic Patent Application Fee Transmittal				
Application Number:		14617787		
Filing Date:		09-Feb-2015		
Title of Invention:		MOBILE MALWARE DETECTION AND USER NOTIFICATION		
First Named Inventor/Applicant Name:		Rainer Baeder		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-012700		
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:				
APPEAL FORWARDING FEE	1413	1	2240	2240
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2240

Electronic Acknowledgement Receipt	
EFS ID:	34084108
Application Number:	14617787
International Application Number:	
Confirmation Number:	1008
Title of Invention:	MOBILE MALWARE DETECTION AND USER NOTIFICATION
First Named Inventor/Applicant Name:	Rainer Baeder
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-012700
Receipt Date:	23-OCT-2018
Filing Date:	09-FEB-2015
Time Stamp:	10:58:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 2240
RAM confirmation Number	102318INTEFSW10592400
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	Fee Worksheet (SB06)	fee-info.pdf	30373	no	2
			211fb085f83432a87ea57054ffc84c58cd9e36a		
Warnings:					
Information:					
Total Files Size (in bytes):			30373		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/617,787	02/09/2015	Rainer Baeder	FORT-012700	1008
64128 7590 11/06/2018 MICHAEL A DESANCTIS HAMILTON DESANCTIS & CHA LLP 12640 W. Cedar Drive, Suite 1 LAKEWOOD, CO 80228 UNITED STATES OF AMERICA			EXAMINER ABRISHAMKAR, KAVEH	
			ART UNIT 3649	PAPER NUMBER
			NOTIFICATION DATE 11/06/2018	DELIVERY MODE ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesantis@hdciplaw.com



United States Patent and Trademark Office

**Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office**

**P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov**

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP Appeal No: 2019-000607
12640 W. CEDAR DRIVE, SUITE 1 Application: 14/617,787
LAKEWOOD, CO 80228 Appellant: Rainer Baeder et al.

Patent Trial and Appeal Board Docketing Notice

Application 14/617,787 was received from the Technology Center at the Board on November 02, 2018 and has been assigned Appeal No: 2019-000607.

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

The mailing address for the Board is:

PATENT TRIAL and APPEAL BOARD
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VIRGINIA 22313-1450

Telephone inquiries can be made by calling 571-272-9797 and referencing the appeal number listed above.

By order of the Patent Trial and Appeal Board.

EMS



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.
14/617,787	02/09/2015	Rainer Baeder	FORT-012700	1008
64128 7590 07/29/2019 MICHAEL A DESANCTIS JAFFERY WATSON MENDONSA & HAMILTON LLP 7501 Village Square Drive, Ste. 206 Castle Pines, CO 80108			EXAMINER ABRISHAMKAR, KAVEH	
			ART UNIT 3649	PAPER NUMBER
			NOTIFICATION DATE 07/29/2019	DELIVERY MODE ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
mdesantis@hdciplaw.com
mike.desantis@jwmhlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte RAINER BAEDER

Appeal 2019-000607
Application 14/617,787
Technology Center 3600

Before JILL D. HILL, LEE L. STEPINA, and ARTHUR M. PESLAK,
Administrative Patent Judges.

STEPINA, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Rainer Baeder (“Appellant”) appeals under 35 U.S.C. § 134(a) from the Examiner’s final decision rejecting claims 1–31. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

CLAIMED SUBJECT MATTER

The claims are directed to mobile malware detection and user notification. Claim 1, reproduced below, is illustrative of the claimed subject matter:

1. A method comprising:
detecting, by a malware detection gateway device associated with a network of a mobile service provider, a malware event based on a data stream transmitted to or from a portable computing device communicating with a packet data network via the network; and
responsive to said detecting, causing a malware reporting/notification message to be sent to a user of the portable computing device in real-time, by sending, by the malware detection gateway device, a malware indicating message to a lookup device, wherein the malware indicating message comprises an Internet Protocol (IP) address of the portable computing device, wherein the malware reporting/notification message (i) includes information regarding a remedial action that can be taken by the user to neutralize malware associated with the detected malware event or a link to the information and (ii) specifies a timeframe within which the user must perform the remedial action or risk deactivation of wireless service provided to the portable computing device by the mobile service provider.

REFERENCES

The prior art relied upon by the Examiner in rejecting the claims on Appeal is:

Rieschick	US 2012/0233656 A1	Sept. 13, 2012
Ramprasad	US 2014/0128020 A1	May 8, 2014
Gupta	US 2014/0189861 A1	July 3, 2014
Qureshi	US 9,378,359 B2	June 28, 2016
Gleichauf	US 9,436,820 B1	Sept. 6, 2016

REJECTION

Claims 1–31 are rejected under 35 USC § 103 as unpatentable over Gupta, Rieschick, Gleichauf, Qureshi, and Ramprasad.

OPINION

The Examiner finds that Gupta discloses many of the elements of claim 1, including detecting a malware event and notifying a user, but relies on Rieschick and Gleichauf to disclose countermeasures to be taken by the user device, and relies on Qureshi and Ramprasad to disclose taking countermeasures within a time period. Final Act. 8–33. The Examiner considers that it would have been obvious to provide a time frame in Gupta for the user to take countermeasures, “so that the user can have an opportunity to engage in a remedial action before the network connection is deactivated.” *Id.* at 29.

Appellant makes arguments for the patentability of claims 1–31 as a group. Br. 11–22. We select claim 1 as representative of the group. *See* 37 C.F.R. § 41.37(c)(1)(iv).

Analogous Art

Appellant argues that Gleichauf, Qureshi and Ramprasad are non-analogous art because they are in fields different than that of the claimed invention and are not pertinent to the particular problem addressed by the inventor. Br. 12–17. Specifically, Appellant takes issue with the Examiner’s position that the relevant field is “network security.” Br. 13. According to Appellant, that is too broad of a concept, and the proper field of endeavor is “a malware detection methodology applicable to mobile

devices.” Br. 15. Appellant asserts that the particular problem “relates to **the difficulties of performing malware scanning on mobile devices.**” Br. 16. Appellant contends that that the problem in both Gleichauf and Qureshi is determining whether it is safe to connect a device to the network, and that the problem in Ramprasad is metering usage in a wireless device. *Id.* For the reasons set forth below, we are not apprised of error in the Examiner’s findings.

Gleichauf

The Examiner finds that Gleichauf determines whether a device is safe in order to minimize the risk of a device transmitting malware. Ans. 4. The Examiner concludes that Gleichauf is reasonably pertinent to the problem with which the inventor was concerned inasmuch as “both Gleichauf and the claimed invention are directed to reducing the possible effect of malware on devices.” *Id.*

Our reviewing court has set forth a two-prong test for determining whether a prior art reference is analogous: (1) whether the reference is from the same field of endeavor as the claimed invention, and (2) if the reference is not within the same field of endeavor, whether the reference is reasonably pertinent to the particular problem with which the inventor is involved. *In re Klein*, 647 F.3d 1343 (Fed. Cir. 2011). The determination that a prior art reference is analogous art is an issue of fact. *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1378 (Fed. Cir. 2007). Although Appellant asserts that the Examiner’s stated field of “network security,” is too broad, Appellant, under the heading “Field,” discloses that “[e]mbodiments of the present invention generally relate to the field of computer networks.” Spec. ¶ 2.

Moreover, although Appellant argues that network security includes many diverse fields and that networks are subject to different types of attacks, it is unclear how this removes Gleichauf, Qureshi, and Ramprasad from Appellant's field of endeavor. Specifically, the structure and function of Gleichauf's network security is to detect "the real-time security state of the computerized device" for "minimizing the risk that the network resources receive malware." Gleichauf 8:21–28. In Gleichauf, the computerized devices include mobile devices, namely, "IP-enabled and cellular telephones, personal digital assistants (PDA's)." *Id.* at 8:40–43. As such Appellant's assertion that Gleichauf is not in the field of "malware detection methodology applicable to mobile devices" (Br. 15) is not persuasive.

Furthermore, Appellant does not persuasively argue that Gleichauf is not pertinent to the problem addressed by Appellant's invention. Specifically, Appellant's assertion that "Gleichauf is not concerned with addressing the difficulties of performing malware scanning on mobile devices," is not well taken. Br. 16. We decline to narrowly define the problem addressed by the inventor to be synonymous with the field of invention inasmuch as this would ignore the fact that the test for determining whether a reference is analogous art has two distinct prongs. *See Klein*, 647 F.3d at 1349. A problem with which the inventor was involved is detecting and responding to malware events associated with mobile/portable computing devices. Spec. ¶ 7. Gleichauf discloses a system that "detects the real-time security state of the computerized device prior to providing the computerized device with access to the network resources, thereby limiting at-risk or vulnerable computerized devices from accessing the network resources and minimizing the risk that the network resources receive

malware.” Gleichauf 8:22–28; *see also id.* at 3:30–49; Ans. 4. Gleichauf discloses that the computerized device includes “IP-enabled and cellular telephones, personal digital assistants (PDA’s), etc. *Id.* at 8:42–43. Gleichauf also discloses “receiving a quarantine message causing the computer system to be reconfigured to more fully comply with required security policy prior to being able to communicate within the network.” *Id.* at 5:26–29. As such, Gleichauf detects and responds to malware events and does so for a mobile device and is, therefore, reasonably pertinent to the inventor’s problem.

Qureshi

In response to Appellant’s assertion that Qureshi is non-analogous art, the Examiner finds that Qureshi’s system is reasonably pertinent to the inventor’s problem because it controls mobile device access based on “conditions indicative of detecting malware and would prevent the execution of an application as a result.” Ans. 4 (citing Qureshi 96:51–60).

Given that Qureshi “relates generally to mobile computing devices (smartphones, tablets, PDAs, etc.) and associated application programs” (Qureshi 1:18–20), which include “an application running therein based on detecting certain conditions, such as conditions indicative of the application having a virus or being malware,” (*id.* at 96:51–54), Appellant’s assertion that Gleichauf is not in the field of “malware detection methodology applicable to mobile devices” (Br. 15) is not persuasive.

Furthermore, assuming, for the purpose of argument, that Qureshi’s system for enabling enterprise users to securely access enterprise resources using their mobile devices to prevent malware and viruses from infecting

other enterprise resources is outside Appellant's field of endeavor, Appellant's argument that Qureshi is not pertinent to the problem addressed by Appellant's invention is unavailing. Qureshi discloses an application running on a mobile device "detecting certain conditions, such as ... malware," and can be configured "to prevent programs from being executed when certain conditions are detected." Qureshi 96:51–59; *see also* Ans. 4. As such, Qureshi detects and responds to malware events in a mobile device and is, therefore, reasonably pertinent to the inventor's problem.

Ramprasad

Responsive to Appellant's assertion that Ramprasad is non-analogous art, the Examiner finds that Ramprasad's wireless device tracking system "is directed towards the same problem of deactivating wireless services if an improper action (e.g. no tracking client installed) has been realized." Ans. 4.

Ramprasad relates generally to providing "wireless services to wireless devices" and addresses "any provisional, billing, security and data issues that might threaten the health of their networks." Ramprasad ¶¶ 2, 4. Although Ramprasad does not use the term "malware," because Appellant discloses that "[m]alware typically refers to undesired code, software of a file, which may interrupt the normal functioning of a device" (Spec. ¶ 3), Appellant does not explain persuasively why detection of improper usage (abnormal functioning) of a mobile device is not within Appellant's field of endeavor.

Moreover, although we appreciate Appellant's position that Ramprasad relates to a tracking client to meter wireless service usage (Br. 17 (citing Ramprasad ¶ 15)), Appellant fails to explain adequately why

“deactivating wireless services if an improper action (e.g. no tracking client installed) has been realized” (*see* Ans. 4), is not pertinent to Appellant’s problem, as the Examiner finds.

A reference is reasonably pertinent if . . . it is one which, because of the matter with which it deals, logically would have commended itself to an inventor’s attention in considering his problem. . . . If a reference disclosure has the same purpose as the claimed invention, the reference relates to the same problem, and that fact supports use of that reference in an obviousness rejection.

Innovention Toys, LLC v. MCA Entm’t, Inc., 637 F.3d 1314, 1321 (Fed. Cir. 2011). Here, Appellant provides “an improved malware detection and notification system and method for mobile devices” (Spec. ¶ 6), because “security of mobile computing devices is weaker than that of laptops and like devices” (*id.* ¶ 4). Under the heading “Related Art,” Ramprasad discloses that wireless networks must “address any provisional, billing, security and data issues that might threaten the health of their networks.” Ramprasad ¶ 4. Given that Ramprasad deals with the problem of addressing threats to the health of a wireless network, we agree with the Examiner that Ramprasad’s concern with how to protect wireless services if an improper action has been realized logically would have commended itself to an inventor’s attention in considering protecting a mobile device from malware or other improper content as in Appellant’s invention. Although the focus of Ramprasad’s disclosure may not be in Appellant’s narrowly defined field of endeavor, it is reasonably pertinent to the problem addressed by the Appellant because it describes similar mobile device protection.

Accordingly, each of Gleichauf, Qureshi, and Ramprasad is properly relied on by the Examiner for establishing obviousness under 35 U.S.C. § 103(a).

Reporting/Notification Message

Appellant also argues that Gupta does not disclose a “malware reporting/notification message,” because in Gupta’s system, “a mobile service provider **may choose to educate subscribers . . . on [sic] their particular behaviors.**” Br. 19 (citing Gupta ¶ 33). Appellant contends that the Examiner’s reliance on Gupta’s reporting module 44 is misplaced because module 44 stores network event information in an event database and “**allow[s] subscribers visibility into the event database 46.**” *Id.* (citing Gupta ¶ 59). Thus, according to Appellant, Gupta does not include a “malware reporting/notification message,” because Gupta merely allows subscribers to access stored network event information. *Id.*

The Examiner responds that Gupta discloses network events, which include detecting malware, creates network event information, and uses a reporting module which provides the event information to the subscriber (user of the mobile device). Ans. 5 (citing Gupta ¶¶ 54, 55, 59). The Examiner notes, moreover, that Rieschick was also relied upon for detecting malware in real-time and alerting a user. *Id.* (citing Rieschick ¶ 29).

Appellant’s arguments are not persuasive. As the Examiner correctly notes, Gupta discloses that “data packets that are being sent to or from subscriber device 12 . . . can be examined . . . to identify any network events[, which] can include malicious software (‘malware’).” Gupta ¶ 54. The “network event data 37 may be provided to correlation module 36,” which provides information that may “include an alert to one or more email

addresses, phone numbers, computers, or other devices.” *Id.* ¶¶ 55–56. Gupta also discloses that the event information from correlations module 36 may be used to generate behavior profiles 50 that may include “attacks sent and received from the subscriber mobile device,” and that reporting module 44 can “provide behavior profiles 50 to the mobile service provider or *subscriber* based on the event information and/or the subscriber device information.” *Id.* ¶¶ 58–59 (emphasis added). Thus, a preponderance of the evidence supports the Examiner’s finding that Gupta sends a “malware reporting/notification message” (alert) to the user.

Rieschick discloses that “various embodiments may detect transmissions of known and unknown malware in real time,” and that “[v]arious embodiments may alert wireless device users of detected malware.” Rieschick ¶ 29; *see also* Final Act. 13. Thus, a preponderance of the evidence supports the Examiner’s finding that Rieschick sends a “malware reporting/notification message” (alert) to the user in real time.

Moreover, nonobviousness cannot be established by attacking the references individually when the rejection is predicated upon a combination of prior art disclosures. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). For the reasons set forth above, the Examiner’s findings are supported by a preponderance of the evidence, and we agree with the Examiner that the combined teachings of Gupta and Rieschick “disclose responsive to said detecting, causing a malware reporting/notification message to be sent to a user of a portable computing device in real-time.”

Ans. 5.

Timeframe for Remedial Action/Hindsight

Appellant argues that the references do not suggest the claim 1 requirement that “the malware reporting/notification message . . . **specifies a timeframe within which the user must perform the remedial action** or risk deactivation of wireless service.” Br. 20. Appellant asserts that the Examiner mischaracterizes the teachings of Gupta and Rieschick because there is no remediation in Gupta, and Rieschick only detects “transmissions of known and unknown malware in real time,” but does not suggest that the detecting and the alerting are connected such that the alerting is also in real time. *Id.* (citing Rieschick). Appellant concludes that a timeframe for remedial action is not supported by the teachings of the references, “but rather appear to be after-the-fact justifications based on Applicant’s disclosure in an exercise of impermissible hindsight.” Br. 21–22.

In response, the Examiner reiterates that the combined teachings of Gupta and Rieschick suggest detecting malware and alerting the wireless users of malware, as well as providing prevention information (countermeasures) to the devices in real time. Ans. 6. The Examiner concludes that because Gleichauf performs a check to determine whether remediation has been performed to ensure access and Qureshi teaches that the remedial action must be performed in a specified time period, the combined teachings of the references suggest “specifying a timeframe within which the user must perform the remedial action in the context of the claim as a whole.” Ans. 8.

Appellant’s arguments are not persuasive. Rieschick discloses that “various embodiments may send detection and prevention information to telecommunications network operators, *wireless devices* and/or malware systems in real time.” Rieschick ¶ 32 (emphasis added); *see also* Ans. 6.

Given that Rieschick discloses detecting and alerting in real time, the Examiner has a sound basis for combining Rieschick with Qureshi to alert a user that if remedial action is not performed in “a specified time period,” the user risks deactivation of “the network connection capability.” Qureshi 62:32–48; *see also* Ans. 7. The Examiner has provided reasoning to support the combination, namely, “so that the user can have an opportunity to engage in a remedial action before the network connection is deactivated.” Final Act. 29. This improvement is disclosed in the cited references, rather than stemming from impermissible hindsight. *See* Qureshi 62:9–57.

We have considered all of Appellant’s arguments regarding claim 1, but find them unavailing. We sustain the rejection of claim 1. Claims 2–31 fall with claim 1.

DECISION

The Examiner’s decision to reject claims 1–31 is affirmed.

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

AFFIRMED



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.
14/617,787	02/09/2015	Rainer Baeder	FORT-012700	1008
64128	7590	10/10/2019		
MICHAEL A DESANCTIS JAFFERY WATSON MENDONSA & HAMILTON LLP 7501 Village Square Drive, Ste. 206 Castle Pines, CO 80108			EXAMINER ABRISHAMKAR, KAVEH	
			ART UNIT	PAPER NUMBER
			3649	
			NOTIFICATION DATE	DELIVERY MODE
			10/10/2019	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
mike.desanctis@jwmhlaw.com

<i>Notice of Abandonment</i>	Application No.	Applicant(s)
	14/617,787	Baeder, Rainer
	Examiner	Art Unit
	KAVEH ABRISHAMKAR	3649

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

This application is abandoned in view of:

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

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

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

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

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

6. ☒ The decision by the Board of Patent Appeals and Interference rendered on 29 July 2019 and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☐ The reason(s) below:

/KAVEH ABRISHAMKAR/ Primary Examiner, Art Unit 3649	
--	--

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