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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2010 (29.04.2010)

PCT

(10) International Publication Number
WO 2010/048220 A1

(51) International Patent Classification:
G06F 15/173 (2006.01)

(21) International Application Number:
PCT/US2009/061372

(22) International Filing Date:
20 October 2009 (20.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/255,621 21 October 2008 (21.10.2008) US

(71) Applicant *(for all designated States except US)*: **FLEXILIS INC.** [US/US]; 639 South Spring Street, #6b, Los Angeles, CA 90014 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MAHAFFEY, Kevin** [US/US]; 11206 Spencerport Way, San Diego, CA 92131 (US).

(74) Agent: **DERGOSITS, Michael, E.**; Dergosits & Noah LLP, Suite 1150, Three Embarcadero Center, Suite 410, San Francisco, CA 94111 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

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

(54) Title: SYSTEM AND METHOD FOR ATTACK AND MALWARE PREVENTION

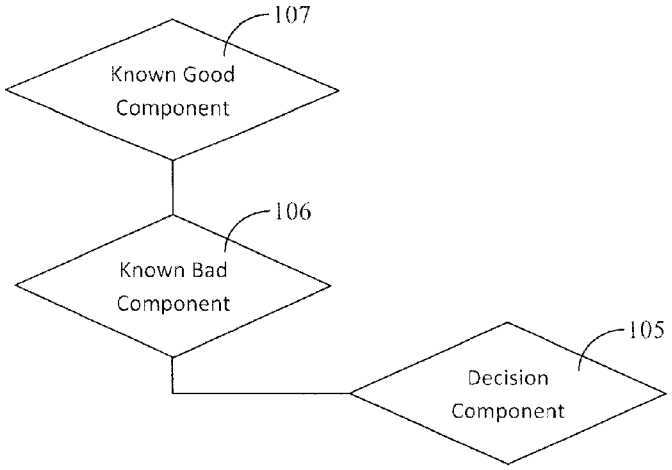

FIG. 1

(57) Abstract: The present invention is a system and method for detecting and preventing attacks and malware on mobile devices such as a cell phones, smartphones or PDAs, which are significantly limited in power consumption, computational power, and memory. The invention enables mobile devices to analyze network data, executable data files, and non-executable data files in order to detect and prevent both known and unknown attacks and malware over vectors that are not typically protected by desktop and server security systems. Security analysis is performed by a combination of "known good," "known bad," and decision components. The invention identifies known good executables and/or known characteristics of network data or data files that must be present in order for the data to be considered good. Furthermore, known good and known bad identifier databases may be stored on a server which may be queried by a mobile device.

WO 2010/048220 A1

SYSTEM AND METHOD FOR ATTACK AND MALWARE PREVENTION

CLAIM OF PRIORITY

This international patent application claims priority under PCT Rule 4.10 and PCT Article 8 to U.S. Patent Application No. 12/255,621, filed on October 21, 2008 at the United States Patent and Trademark Office, and which is hereby incorporated by reference.

FIELD

The present invention relates generally to data security, specifically, to preventing and detecting attacks on a mobile communications device.

BACKGROUND

There are many ways for protecting computing assets from the harmful effects of viruses, malware, adware, exploits, and other computer contaminants (also known collectively as "attacks"). Desktop, laptop and server computers enjoy numerous antivirus, network, and similar security software products that are able to detect security threats such as exploits, viruses, and malware. The detection of known viruses and malware often involves identifying the software code signatures or definitions of known viruses and malware, storing these signatures or definitions in a database on the computer, and comparing data with these signatures or definitions in order to determine whether or not the data contains a virus or malware. Detecting previously unknown viruses and malware may often involves analyzing data for certain characteristics or emulating the execution of data to determine what it would do if allowed to run on the host system. Identifying new attacks is a matter of updating a virus definition or virus signature database on the computer or modifying the rules associated with an unknown virus/malware detection system. This is feasible since computers have the hardware, software and memory resources to store and manage vast virus signature databases, as well as the processing resources to perform complicated analyses and emulate an execution environment. The detection of exploits or other attacks that can compromise a computer via a network often involves identifying the signatures of known exploits or attack, storing a database of signatures on the computer being protected, and comparing network data to these signatures in order to determine if the data contains a security threat. Like virus and malware signatures, network attack signatures can be updated in order to detect new security threats. As mentioned previously, such a system is made possible because computers have the

computational and storage resources available to manage large attack signature databases and compare network data to many signatures before approving it.

Mobile communications devices lack the same power as computers, though they are often designed to provide some of the same functionalities as computers in a portable form. In order to provide these functionalities, mobile communications devices often retain a mobile or portable version of a desktop computer operating system or system architecture, such as Windows Mobile®, Apple OS X iPhone™ or Java® ME. As a result, some attacks directed to a traditional computer can easily translate or be modified to harm a mobile communications device. Additionally, the number and types of attacks specifically directed to the mobile communications device platform is growing.

Detecting attacks on a mobile communications device presents challenges not found on traditional computing platforms. As previously mentioned, mobile communications devices lack the hardware, software and memory resources of a traditional computer. As such, storing vast signature databases on the mobile communications device is not feasible, and running complicated analysis systems strains the device's memory, battery, and CPU. Other security solutions have been found unsuccessful at detecting attacks specifically directed to a mobile communications device, since mobile communications devices provide functionalities not found on traditional computers. For example, a mobile communications device may be attacked via network data, files, or executables received over various network interfaces such as Bluetooth, Wi-Fi, infrared, or cellular networks.

The lack of robust antivirus and attack preventative measures on mobile communications devices has serious security implications. Mobile devices are part of a critical infrastructure: as people depend on such devices to communicate, transmit and receive data, and access Internet and intranet websites, it becomes more important that these devices remain secure. If not protected, a significant portion of mobile devices may be vulnerable to criminal or cyber-terrorist attacks that could disrupt the normal functioning of both commerce and government. One skilled in the art could easily disrupt vital communications, use mobile communications devices to hack into supposedly secure servers storing confidential information, steal money via mobile payment mechanisms, or perform a host of other malicious and nefarious acts.

What is therefore needed is a way to prevent attacks and protect mobile communications devices without sacrificing device performance.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

Figure 1 is an exemplary block diagram depicting one embodiment of the present invention.

Figure 2 is an exemplary flow diagram illustrating the steps of an embodiment of the present invention.

Figure 3 is an exemplary flow diagram illustrating the steps of an embodiment of the present invention.

DETAILED DESCRIPTION

The present invention is a system and method for evaluating data on a mobile communications device to determine if it presents a security threat. In an embodiment, the present invention provides a mobile communications device with a mechanism for rejecting data that is immediately recognized to be an attack, and for allowing receipt of data recognized to be safe. In addition, the present invention provides a way for the mobile communications device to evaluate data that is not immediately recognized as safe or malicious. The present invention functions on a mobile communications device notwithstanding any hardware, software or memory constraints inherent in the device. As used herein, a "mobile communications device" may refer to a cell phone, handset, smartphone, PDA, and the like. A mobile communications device may primarily be used for voice communications, but may also be equipped to receive and transmit data, including email, text messages, video, and other data. This data may be received as packets or streams.

It should be appreciated that the present invention can be implemented in numerous ways, including as a process, an apparatus, a system, a device, a method, or a computer readable medium such as a computer readable storage medium comprising computer program instructions or a computer network wherein computer program instructions are sent over optical or electronic communication links. Applications, software programs or computer readable instructions may be referred to as components or modules. Applications may take the form of software executing on a general purpose computer or be hardwired or hard coded in hardware. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention.

A. System Architecture

In an embodiment, the present invention is comprised of at least three software components resident on a mobile communications device. As shown in Figure 1, a first component 107 may be used to recognize data that is safe, or "known good." A second component 106 may be used to recognize data that is malicious, or "known bad." A third component 105 is a decision component that may be used to evaluate data that is neither known good nor known bad. Each of these components is discussed in more detail below.

One will appreciate that as referred to herein, data may include network data, files, executable and non-executable applications, emails and other types of objects that can be

transmitted to or received by a mobile communications device. Mobile communications devices typically transmit and receive data through one or more network interfaces, including Bluetooth, WiFi, infrared, radio receivers, and the like. Similarly, data may be encapsulated in a layered communications protocol or set of protocols, such as TCP/IP, HTTP, Bluetooth, and the like. In order to evaluate the security threat level of the data, it may be necessary to identify or parse the one or more protocols used to encapsulate the data. This may be done using a system such as the one described in co-pending U.S. Patent Application No. 12/255,614, entitled "SYSTEM AND METHOD FOR MONITORING AND ANALYZING MULTIPLE INTERFACES AND MULTIPLE PROTOCOLS," which is incorporated in full herein.

In addition, one will appreciate that data can vary in size and complexity depending upon its source, destination and purpose. It may be difficult to analyze received data objects as a whole; therefore, in order to optimize resources on the mobile communications device platform, the present invention may apply hashing functions or hashing algorithms to the received data. A hashing algorithm will transform the data into a fixed length identifier for easier evaluation. Applying the hash function may be performed by any of the components in the system illustrated in figure 1, or alternatively, may simply be performed by the system itself.

Hashed data may then be submitted to some or all of the three components for categorization and further action, if necessary. For example, the known good component 107 may have access to or may associate with a stored database of known good hash identifiers. As discussed herein, the database may be a data store or table of known good hash identifiers, or may be logic providing a comparison against hash identifiers for known good data. When data is analyzed by the mobile communications device, it may be quickly hashed and compared against this stored database by the known good component. This database may include identifiers for data that has been analyzed before and been deemed safe, originates from a trustworthy source, or simply recognized as good based upon its characteristics. This may include an examination of the data's structure, statefulness, purported source and destination, etc. If there is a match against the known good hash identifier database, then the data may be categorized as known good, and no further analysis is necessary. This data may then be allowed to pass to its intended destination for processing, execution or other operation.

A person skilled in the art will appreciate that since the total number of known good applications for mobile communications devices is small, use of the known good component 107 coupled to a database of known good application identifiers may significantly reduce false-positive malware detection. One will also appreciate that use of a known good component 107 may be particularly effective for data that contains executable software code. Executable software code for a given application rarely changes between different mobile communications devices, so creating a database of known good hash identifiers or logic for evaluating known good hash identifiers may be an effective method for recognizing safe or trustworthy data. This database may vary in size depending upon the resources available on the mobile communications device. Alternatively, aspects of the present invention, such as the known good component, may have access to a remote server with a larger library of hash identifiers for known good data or applications. Additionally, as discussed further in the next section, known good component 107 may be able to evaluate the security of data depending upon whether the data possesses sufficient characteristics common to other known good data.

The second component of the system embodiment of the present invention may include a component capable of recognizing if received data is malicious, or "known bad" (106 in Figure 1). Known bad component 106 may have access to a database, logic or other data store containing information on known attack signatures or definitions that can be stored on the mobile communications device without occupying a significant amount of memory. For example, virus or other malware signatures can be reduced to hashing identifiers and stored in a database. In other words, there may be a known bad hash identifier database that complements the known good hash identifier database stored on the mobile communications device. Additionally or alternatively, known bad component 106 may be capable of identifying malware using characteristics common to other malicious software code. When applied to network data or data files, known bad component 106 may have access to a database containing patterns or other characteristics of a protocol data unit or file format which presents a security threat. Similar to the known good component 107 and database, any data identified as containing malware may be deleted, quarantined, or rejected from further processing by the mobile communications device. If a known bad data object is detected, the present invention may also display a notification or other message similar to that described in co-pending U.S. Patent Application No. 12/255,635, entitled "SECURITY STATUS AND INFORMATION DISPLAY SYSTEM," incorporated in full herein.

The third component of the system embodiment of the present invention may be a decision component 105. This component may be used to evaluate data that cannot be characterized as either known good or known bad. Since a majority of the data received on the mobile communications device may fall within this category, this component may utilize most of the resources allocated to the system embodiment of the present invention. This component may apply fuzzy logic, heuristic or other methods of analysis in order to determine whether received data may be passed to its intended destination, or rejected to prevent harm from befalling the device. Examples of this analysis are discussed below.

One will appreciate that the system embodiment may exist independently on a mobile communications device, or may be incorporated into an existing security system on the mobile communications device such as the one in co-pending U.S. Patent Application No. [1129.06]. One will also appreciate that in order to implement the present invention on a variety of mobile communications device platforms, it may be necessary to program aspects of the present invention using a cross-platform system, such as the one disclosed in co-pending U.S. Patent Application No. 12/255,626, entitled "SYSTEM AND METHOD FOR A MOBILE CROSS PLATFORM SOFTWARE SYSTEM," incorporated in full herein. In addition, aspects of the present invention may be used to determine a security state for a mobile communications device, as is described in co-pending U.S. Patent Application No. 12/255,632, entitled "SECURE MOBILE PLATFORM SYSTEM," incorporated in full herein.

One will also appreciate that while the present invention is disclosed as installed on a mobile communications device, portions of the present invention may communicate or work in conjunction with a remote server or a series of servers. For example, the system embodiment of the present invention may be configured to update its virus definitions or compare received data against a larger virus signature database on a remote server. Alternative, the mobile communications device may be configured to send a hash identifier for received data to one or more servers for analysis and/or evaluation. One server may contain the known good component 107, known bad component 106 and decision component 105 of the present invention, or the components may be distributed across two or more servers. The one or more servers may thereby perform the analysis using the hash identifier, and if analysis reveals that the hash identifier identifies recognizably safe data, then the one or more servers may notify the mobile communications device or instruct the device that it may accept and process the data. If the analysis reveals that the hash identifier identifies

recognizably malicious data, then the one or more servers may notify the mobile communications device or instruct the device to reject the data and not process it further. If the analysis is inconclusive, then the one or more servers may request that the mobile communications device send the data identified by the hash identifier to a server for further analysis. Further analysis may be performed by a decision component 105 or manually. One will appreciate that other variations are possible without departing from this disclosure or the scope of the present invention.

B. Malware and Attack Detection Using Data Characteristics

The system architecture discussed above offers an improvement over prior art mobile communications device security systems that typically only include a known good detection method or a known bad detection method. Because the present invention incorporates a decision component 105 as well, it minimizes false-positive or false-negative detection errors common to prior art systems. Other advantages and improvements are discussed in this section that describes some of the analyses performed by the system embodiment of the present invention.

1. Known Good Characteristics

In an embodiment, the present invention may be configured to recognize good characteristics that all known good data should possess. Analyzing data for good characteristics may include the equivalent of applying a database or other data store of known good characteristics or logic asserting known good characteristics, and performing a comparison against the database. Alternatively or additionally, analyzing data for good characteristics may include the equivalent of applying logic asserting known good characteristics. The database or logic may not include all of the characteristics that may determine if data is good; however, if the data object lacks key known good characteristics, then the system can conclude that the data may be malicious and should be further analyzed, or alternatively, rejected outright. The database of known good characteristics or logic asserting known good characteristic may supplant the known good component 107 discussed above, or in some cases may replace it as a lightweight alternative. In other words, a list of all the known good data files and network data may be infinitely large, but the list of characteristics common to known good data files and known good network data may be much smaller. As such, the database of known good characteristics may be smaller in size than the

known good database, and may therefore be more practical in mobile communications devices with less memory or processing resources.

One will appreciate that there are a number of characteristics common to known good data, but that these characteristics may differ depending upon whether the data is network data, a data file, or executable data. The present invention is able to evaluate all types of data receivable by a mobile communications device. For example, network data and data files may be examined for structure and state. This may involve checking the data against its associated metadata to confirm that the size, type and description match the data being described. Using this analysis, known good component 107 may be configured to allow or accept data that has valid statefulness and structure, and provide data that does not pass these tests to the known bad component 106 for further analysis or simply reject it outright. One will appreciate, however, that having valid statefulness and structure are not alone enough for concluding that a data file or network data is good, and further analysis by known bad component 106 and/or decision component 105 may be necessary. In other words, even though data analyzed by known good component 107 may result in a positive match finding that the data has recognizably good characteristics, or has a hash identifier matching known good data, the data may still be analyzed by known bad component 106 and/or decision component 105.

With regards to executable data, the list of known good executable applications for mobile communications devices is small. As such, known good component 107 may simply compare hash identifiers for gathered executable data and compare them against a stored database of known good executables. One will appreciate that other methods, such as validating the structure of an executable file format or validating any cryptographic signatures on an executable may be applied as well.

2. Known Bad Characteristics

In an embodiment, data may be compared using logic or a database or other data store of known bad characteristics. As such, if data has known bad characteristics, it may be considered malicious and may be rejected, deleted or quarantined. One will appreciate that the entire data object may have known bad characteristics, or part of the data object may have known bad characteristics, or a pattern in an object may be recognized as known bad, or the data object may yield a positive result from logic that performs a specific test for known bad characteristics. In such situations, it may warrant further analysis or confirmation to avoid an inaccurate result. Further analysis protects against situations in which the present invention may not recognize a specifically malicious data object that has not been recognized as such

before. It is preferable to avoid mistakenly characterizing an object as more good than bad if it presents a security threat. Data that is recognized as known good, or is recognized has having sufficient known good characteristics, may be passed on to its intended destination. Data that fails to have all of the characteristics of a known good file or application, is found to be more bad than good, or is simply unrecognized may be passed along to the decision component 105 for further analysis.

As noted previously, data may be analyzed differently depending upon whether it is network data, file data, or executable data. Network data and file data may be encapsulated in various multi-layer protocols or formats. These protocols or formats may be analyzed using the system and methods described in co-pending U.S. Patent Application 12/255,614. If any of the data has known bad violations of its purported protocol or format, contains anomalous content or state transitions, or is invalid for the processor or subsystem to which it is directed, then known bad component 106 may reject this data as potentially malicious.

Known bad executables may be evaluated using full hash signatures, a string match anywhere or at a relative or absolute offset in the file, or a pattern anywhere or at a certain offset in the file consistent with known pieces or families of malware. If any of these characteristics are encountered, then the known bad component 106 may identify the data as malware and reject it. One will appreciate that other methods for detecting known bad data may be used as well, including but not limited to blocking executables which utilize a piece or specific combination of privileged functionality, or blocking executables which a server deems to have access frequency characteristics across many mobile devices indicative of viruses or malware.

3. Further Analysis

In some instances, data may not be immediately recognized as known good or known bad, and so decision component 105 may be used. One will appreciate that a key aspect of the present invention is its ability to analyze data that is not immediately known good or known bad. As mentioned above, this may require an analysis to determine if data is more good than bad, or more bad than good. As such, the present invention provides a sliding scale with which to assess the degree of how good or how bad received data may be. This permits a more precise measurement of not only how data may or may not harm a mobile communications device, but in light of this data, how the overall security state of the device may change.

The decision component 105 may utilize one or more types of internal decision systems to characterize whether data is good or bad. The decision component 105 is designed to detect security threats without specific signatures for the threats being protected against. In other words, decision component 105 may operate as an additional security component to compensate for any weaknesses from known good component 107 or known bad component 106.

One will appreciate that there are a number of decision systems that may be utilized by decision component 105, including but not limited to heuristic algorithms, rule-based or non-rule-based expert systems, fuzzy logic systems, neural networks, or other systems that may be used to classify a subject. In an embodiment, decision component 105 can analyze network data or files for possible security threats. For example, a fuzzy system may be configured to analyze the timing related to authentication actions over a given protocol, such as Bluetooth. A remote device connected to the local device via Bluetooth may repeatedly try to request access to a privileged resource on a device. Each time the remote device sends an authentication request, a window may pop up on the target device that requires user action before normal device interaction can resume. Because there is often no rate limiting built into the Bluetooth authentication system of mobile phones, a remote device can continue interrupting the local user by requesting access to the privileged resource and until the local user becomes frustrated and simply grants the request.

A fuzzy system can analyze data such as the timings between authentication requests, the results of previous authentication requests, and the time required for the user to respond to previous authentication requests. Such a system can detect when a remote device is attempting to repeatedly request authorization and the user is denying it quickly to prevent a situation where the user becomes frustrated and grants privileged access on his or her device to a remote attacker. Such a system can also be used to detect denial of service attacks, port scans, or other attacks that have a significant temporal component.

In another example, a heuristic algorithm may be used to detect the presence of shellcode in a data packet, stream, or data file in which none is expected. Such shellcode may be indicative that the data contains an exploit designed to perform a memory corruption attack where the attacker aims to have the supplied shellcode executed by the target device's processor.

In another example, the decision component 105 may contain a system for detecting anomalies in protocol behavior or file content so as to catch security threats that rely on unforeseen, yet out-of-the-ordinary mechanisms.

In another example, the decision component 105 may contain a system for analyzing authentication or other strings in network data or files that may be used to "socially engineer" a user. "Social engineering" attacks often manipulate the user into performing an action that is not in his or her best interest by using false information or otherwise presenting information to the user that he or she may interpret as legitimate but, in fact, is not. Such a system can examine the content of strings to determine if the data is of legitimate origin or is a potential social engineering attack. Examples of attacks this type of system may stop include: "phishing," "SMS phishing," Bluetooth device name manipulation, and others.

In an embodiment, the decision component 105 may analyze applications, libraries, or other executables on a mobile communications device. In an example, the decision component 105 may contain a neural network which analyzes characteristics of an executable and determines a security assessment based on pre-set connection characteristics. Such characteristics may be determined based on information contained in the executable file format or as a result of processing the content of the executable file.

In an example, the decision component 105 may contain a virtual machine-based decision system by which an executable can be classified by a set of rules that may be updated independently of the decision component itself. Such a system is able to add new logic to detect certain new classes of viruses on the fly without having to update the whole decision component. The system may pre-process the executable so that the virtual machine's logic can symbolically reference the executable rather than having to process the executable itself.

In an example, the decision component 105 may contain an expert-system which analyzes the behavior of an executable through function calls, system calls or actions an executable may take on an operating system. If an executable access sensitive system calls in a way that signifies malicious behavior, the system may flag that executable as potential malware and action may be taken.

The above examples illustrate how decision component 105 may utilize a number of analytical methods in order to fully evaluate the threat level of data received by or transmitted from the mobile communications device. Other examples may be contemplated without departing from the scope of this disclosure or the spirit of the present invention.

C. Data Analysis

Figures 2 and 3 provide examples of how the system described above may apply its algorithm for evaluating data to detect malware and prevent attack. Figure 2 illustrates the present invention evaluating network data or data files. Figure 3 illustrates the present invention evaluating executable code. Each is discussed in turn.

1. Analysis of Network Data or Data Files

As shown in Figure 2, step 201 may involve gathering data sent to or received from the mobile communications device. The data may be analyzed to identify its protocol and track state (step 203). One will appreciate that these steps may be performed in whole or in part by the system described in co-pending U.S. Patent Application No. 12/255,635. In step 205, known good component 107 may evaluate the gathered data for known good characteristics. Known good characteristics may include the characteristics previously discussed. If the data contains sufficient known good characteristics, it may be allowed to proceed to its intended destination (step 211) for processing, execution or other operation. Alternatively, it may be further analyzed by known bad component 106 to confirm that the data is truly safe (step 207). If known bad component 106 determines that the data is truly safe, then the data may be allowed to proceed to its intended destination (step 211). Decision component 105 may also be available to provide a final check (step 209) before allowing the data to proceed (step 211).

At any point during the analysis, if either known good component 107, known bad component 106 or decision component 105 determines that the data is not good, or affirmatively contains security threats, data inconsistencies, etc., then in step 213 the data will be blocked, rejected, deleted or quarantined. As discussed above, a signal even or security event information log may be updated to record the encounter with the contaminated data.

One will appreciate that the steps illustrated in Figure 2 are merely exemplary and are not meant to limit the present invention to any one method.

2. Analysis of Executable Data

Like Figure 2, Figure 3 similarly depicts and exemplary method for evaluating executable data, including but not limited to applications, programs and/or libraries on the mobile communications device. In step 301, the executable is determined to need to be classified as either good or bad as a result from an attempt to access the executable or the executable being downloaded or otherwise transferred to the mobile device. The executable may or may not be pre-processed to determine a hash identifier or other characteristic before

being evaluated by known good component 107. This evaluation may include comparing the executable's hash identifier against a database of known good characteristics, identifying whether the executable has sufficient known good characteristics, or any of the criteria discussed above. If the executable is recognized as known good, then in step 311, it may be allowed to execute its code or proceed to its intended destination for processing or other operation. If known good component 107 fails to allow the executable data, then known bad component 106 may perform its analysis (step 305). If known bad component 106 confirms that the executable is malicious, then the executable may be quarantined, rejected, or deleted, and the event may be logged (step 309). If known bad component 106 is unable to characterize the executable, then the decision component 105 may perform its analysis as described above (step 307). If decision component 105 ultimately determines that the executable is safe, then the executable is allowed (step 311). If decision component 105 ultimately determines that the executable is not safe, or remains unsure, then the executable may be quarantined (step 309). One will appreciate that since executables may contain code that can cause significant harm to the mobile communications device, it may require more rigorous analysis before the executable is allowed to proceed. Any of the steps illustrated in Figure 3 may be altered without departing from this disclosure or scope of the present invention.

One will appreciate that the above examples contemplate that the present invention operates wholly on a mobile communications device. However, as previously discussed, it is also possible for portions of the present invention to reside on one or more remote servers. In the example of an antivirus system, a file's hash identifier may be transmitted to a remote server that then identifies whether the file is known good or known bad, or if the file contains known good or known bad characteristics. If the server does not recognize the file's hash identifier, the server may request that the file itself be transmitted to the server for analysis. This analysis may be automatic, or may be performed by a human. The server may furthermore analyze access patterns of a given executable between multiple devices to determine if the executable has virus or malware-like spreading characteristics. In an embodiment, analysis on the server is concurrent or in conjunction with an analysis performed by and on the mobile communications device. If the mobile communication device's antivirus system fails to classify the file, it may query the server for its results. Alternatively or in addition, the present invention on the mobile communications device may perform a heuristic analysis using the decision component 105 described above. The results from the local

decision component 105 on the mobile communications device may be logged locally and/or transmitted to the server.

As described above, the present invention provides a robust and flexible security system for preventing attacks on a mobile communications device. By implementing the present invention, attacks from cyber-terrorists and other criminal groups may be thwarted. As a result, mobile communications devices can be used for many tasks with a reduced risk of security threats such as exploits, viruses, malware, social engineering attacks, denial of service attacks, and the like.

One will appreciate that in the description above and throughout, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be evident, however, to one of ordinary skill in the art, that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form to facilitate explanation. The description of the preferred embodiments is not intended to limit the scope of the claims appended hereto.

CLAIMS

What is claimed is:

1. In a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, a method comprising:

providing data on the mobile communications device;

applying a hash function to the data to create a hash identifier for the data; and

comparing by the known good component, the data hash identifier against a database of identifiers of known good data stored in the mobile communications device memory; and

if the comparison by the known good component results in a positive match, then allowing the data to be processed by the mobile communications device.

2. The method of claim 1, further comprising:

if the comparison by the known good component does not result in a positive match, then comparing by the known bad component, the data hash identifier against either a database of identifiers of known bad data stored in the mobile communications device memory, or against a database of known bad data signatures stored in the mobile communications device memory, or against a database of known bad data patterns stored in the mobile communications device memory; and

if the comparison by the known bad component results in a positive match, then rejecting the data from being processed by the mobile communications device.

3. The method of claim 2, further comprising:

if the comparison by the known bad component does not result in a positive match, then using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis determines that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis determines that the data is malicious, then rejecting the data from being processed by the mobile communications device.

4. In a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, a method comprising:

providing data on the mobile communications device;

applying by the known good component, logic on the data to determine if the data is safe;

if the known good component logic determines that the data is safe, then allowing the data to be processed by the mobile communications device;

if the known good component does not determine that the data is safe, then applying by the known bad component, logic on the data to determine if the data is malicious; and

if the known bad component logic determines that the data is malicious, then rejecting the data from being processed by the mobile communications device.

5. The method of claim 4, further comprising:

using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis shows that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis shows that the data is malicious, then rejecting the data from being processed by the mobile communications device.

6. In a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, a method comprising:

providing data on the mobile communications device;

applying by the known good component, logic on the data to determine if the data is safe;

if the known good component logic determines that the data is safe, then allowing the data to be processed by the mobile communications device;

if the known good component logic does not determine that the data is safe, then rejecting the data from being processed by the mobile communications device.

7. The method of claim 6, further comprising:

if the known good component logic does not determine that the data is safe, then applying by the known bad component, logic on the data to determine if the data is malicious; and

if the known bad component logic determines that the data is malicious, then rejecting the data from being processed by the mobile communications device.

8. The method of claim 7, further comprising:

using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis determines that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis determines that the data is malicious, then rejecting the data from being processed by the mobile communications device.

9. In a server connected through a telecommunications network to receive data from and send data to a mobile communications device, the server having a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a method comprising:

by the server, receiving a hash identifier for data from the mobile communications device;

comparing, by the known good component, the data hash identifier against a database of identifiers of known good data stored in memory associated with the server; and

if the comparison by the known good component results in a positive match, then sending an instruction to the mobile communications device to allow the data to be processed by the mobile communications device.

10. The method of claim 9, wherein the server further includes a known bad component for identifying data that is recognizably malicious, the method further comprising:

if the comparison by the known good component does not result in a positive match, then comparing by the known bad component, the data hash identifier against a database of identifiers of known bad data stored in memory associated with the server; and

if the comparison by the known bad component results in a positive match, then sending an instruction to the mobile communications to reject the data from being processed by the mobile communications device.

11. The method of claim 10, wherein the server further includes a decision component for evaluating whether data is safe or malicious, the method further comprising:

if the comparison by the known bad component does not result in a positive match, then receiving the data from the mobile communications device; and

using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis determines that the data is safe, then sending an instruction to the mobile communications device to allow the data to be processed by the mobile communications device; and

if the analysis determines that the data is malicious, then sending an instruction to the mobile communications device to reject the data from being processed by the mobile communications device.

12. In a server connected through a telecommunications network to receive and send data, having a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a method comprising:

receiving data at the server from the mobile communications device;

applying by the known good component, logic on the data to determine if the data is safe;

if the known good component logic determines that the data is safe, then allowing the data to be processed by the mobile communications device;

if the known good component logic does not determine that the data is safe, then rejecting the data from being processed by the mobile communications device.

13. The method of claim 12, wherein the server further includes a known bad component for identifying data that is recognizably malicious, the method further comprising:

if the known good component logic does not determine that the data is safe, then applying by the known bad component, logic on the data to determine if the data is malicious; and

if the known bad component logic determines that the data is malicious, then rejecting the data from being processed by the mobile communications device.

14. The method of claim 13, wherein the server further includes a decision component for evaluating whether data is safe or malicious, the method further comprising:

using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis shows that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis shows that the data is malicious, then rejecting the data from being processed by the mobile communications device.

15. A computer readable medium stored in a memory of a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, the computer readable medium containing computer readable instructions comprising:

computer program code for comparing by the known good component, the data hash identifier against a database of identifiers of known good data stored in the mobile communications device memory;

computer program code for comparing by the known bad component, the data hash identifier against either a database of identifiers of known bad data stored in the mobile communications device memory, or against a database of known bad data signatures stored in the mobile communications device memory, or against a database of known bad data patterns stored in the mobile communications device memory; and

computer program code for performing an analysis on the data by the decision component to determine if the data is safe or malicious.

16. A computer readable medium stored in a server connected through a telecommunications network to receive and send data, having a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, the computer readable medium containing computer readable instructions comprising:

computer program code for comparing by the known good component, the data hash identifier against a database of identifiers of known good data stored in memory associated with the server;

computer program code for comparing by the known bad component, the data hash identifier against either a database of identifiers of known bad data stored in memory associated with the server, or against a database of known bad data signatures stored in memory associated with the server, or against a database of known bad data patterns stored in memory associated with the server; and

computer program code for performing an analysis on the data by the decision component to determine if the data is safe or malicious.

17. In a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, a method comprising:

providing data on the mobile communications device;

comparing by the known good component, the data against a database of characteristics for known good data stored in the mobile communications device; and

if the comparison by the known good component does not result in a positive match, then rejecting the data from being processed by the mobile communications device.

18. The method of claim 17, further comprising:

if the comparison by the known good component results in a positive match, then comparing by the known bad component, the data against either a database of characteristics for known bad data stored in the mobile communications device memory, or against a database of known bad data signatures stored in the mobile communications device memory, or against a database of known bad data patterns stored in the mobile communications device memory; and

if the comparison by the known bad component results in a positive match, then rejecting the data from being processed by the mobile communications device.

19. The method of claim 18, further comprising:

if the comparison by the known bad component does not result in a positive match, then using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis shows that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis shows that the data is malicious, then rejecting the data from being processed by the mobile communications device.

20. In a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, a method comprising:

providing data on the mobile communications device;

applying a hash function to the data to create a hash identifier for the data; and

comparing by the known good component, the data hash identifier against a database of identifiers of known good data stored in the mobile communications device memory; and

if the comparison by the known good component does not result in a positive match, then rejecting the data from being processed by the mobile communications device.

21. The method of claim 20, further comprising:

if the comparison by the known good component results in a positive match, then comparing by the known bad component, the data hash identifier against a database of identifiers of known bad data stored in the mobile communications device memory, or against a database of known bad data signatures stored in the mobile communications device memory, or against a database of known bad data patterns stored in the mobile communications device memory; and

if the comparison by the known bad component results in a positive match, then rejecting the data from being processed by the mobile communications device.

22. The method of claim 21, further comprising:

if the comparison by the known bad component does not result in a positive match, then using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis shows that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis shows that the data is malicious, then rejecting the data from being processed by the mobile communications device.

23. In a mobile communications device having a network interface for receiving and sending data, a memory and a microprocessor, and further having software components for processing, analyzing and storing data, including at least a known good component for identifying data that is recognizably safe, a known bad component for identifying data that is recognizably malicious, and a decision component for evaluating whether data is safe or malicious, a method comprising:

providing data on the mobile communications device;

applying by the known good component, logic on the data to determine if the data is not safe; and

if the known good component logic determines that the data is not safe, then rejecting the data from being processed by the mobile communications device.

24. The method of claim 23, further comprising:

if the known good component logic does not determine that the data is not safe, applying by the known bad component, logic on the data to determine if it is malicious; and

if the known bad component determines that the data is malicious, then rejecting the data from being processed by the mobile communications device.

25. The method of claim 24, further comprising:

using the decision component, performing an analysis on the data by the decision component to determine if the data is safe or malicious;

if the analysis shows that the data is safe, then allowing the data to be processed by the mobile communications device; and

if the analysis shows that the data is malicious, then rejecting the data from being processed by the mobile communications device.

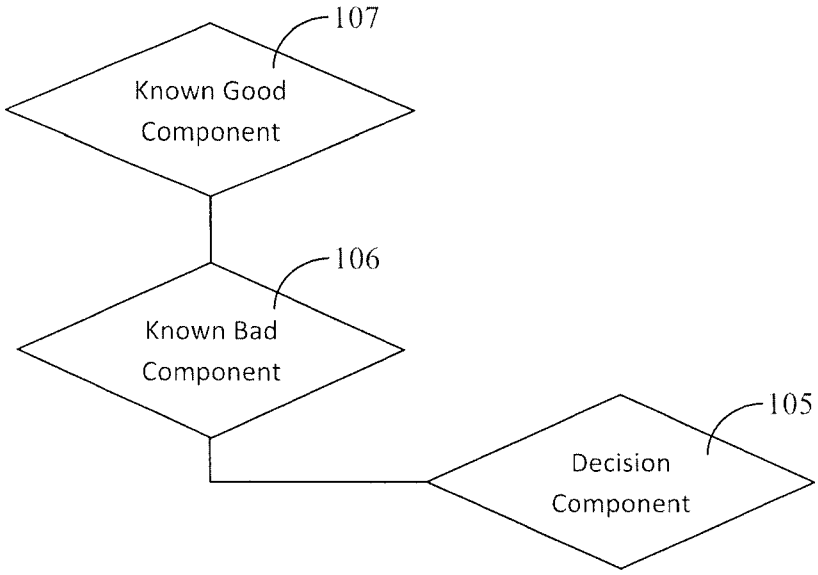
107
Known Good Component
106
Known Bad Component
105
Decision Component

FIG. 1

NETWORK DATA OR DATA FILES

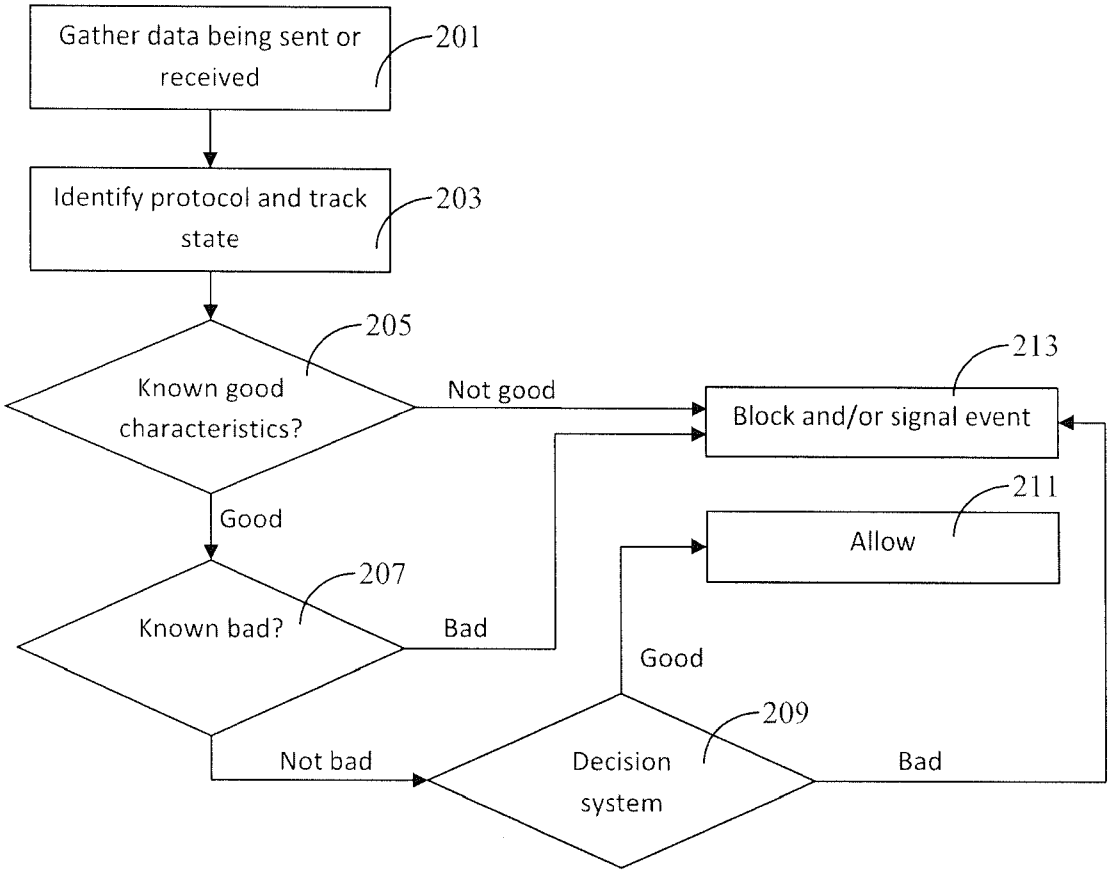

FIG. 2

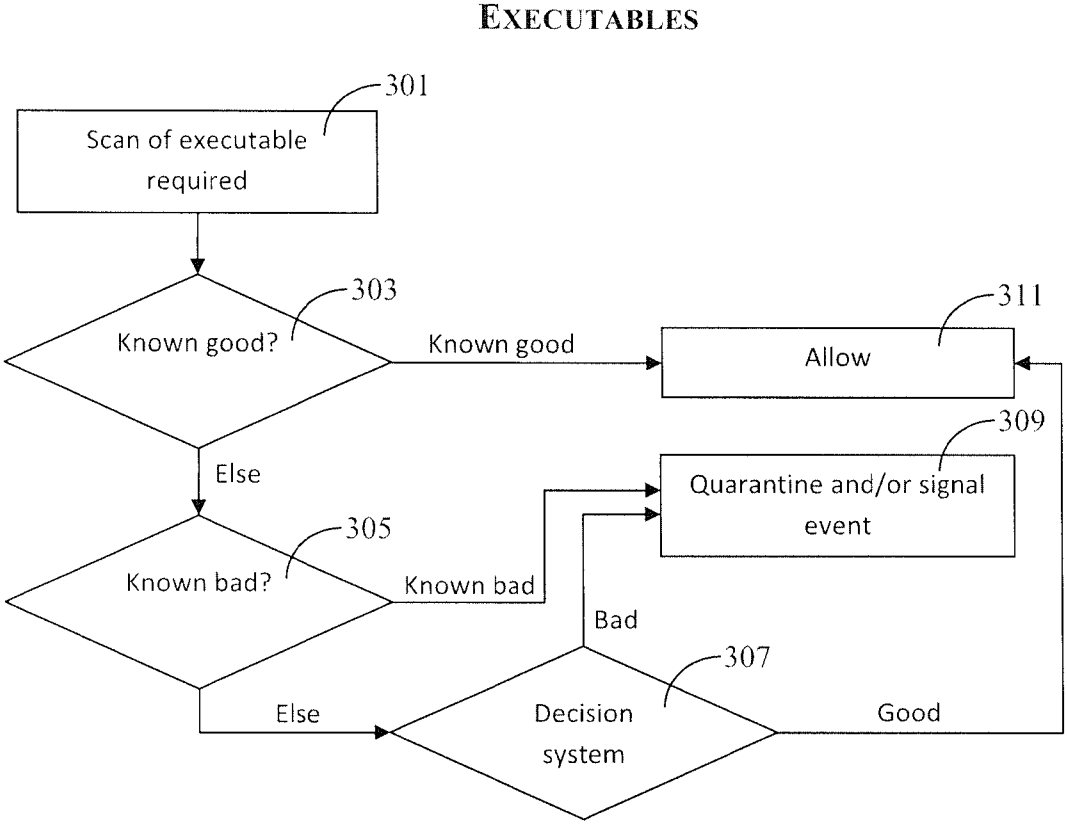
EXECUTABLES
301
Scan of executable required
303
Known good?
Known good
311
Allow
309
Quarantine and/or signal event
Else
305
Known bad?
Known bad
Bad
307
Else
Decision system
Good

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/061372

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 15/173 (2010.01)
USPC - 709/224
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 12/14, 15/173; H04L 29/06 (2010.01)
USPC - 709/224, 225; 713/151-153

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Micropat

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2007/0240218 A1 (TUVELL et al) 11 October 2007 (11.10.2007) entire document	1-8, 15, 17-25 ------- 9-14
X --- Y	US 2003/0115485 A1 (MILLIKEN) 19 June 2003 (19.06.2003) entire document	16 --- 9-14

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 March 2010	24 MAR 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/061372

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/061372

Continuation of Box III.

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-8, 15, 17-25, drawn to a mobile device for evaluating whether data is safe or malicious by comparing the data against known good data and known bad data stored within an internal database of the mobile device
Group II, claims 9-14 and 16, drawn to a server receiving information from a mobile device, and evaluating whether the received data is safe or malicious by comparing the received information against known good data and bad known data stored in the server's memory.

The inventions listed as Groups I-II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: evaluating whether data is safe or malicious by comparing the data against known good data and known bad data stored within an internal database of the mobile device as claimed therein is not present in the invention of Group II. The special technical feature of the Group II invention: a server receiving information from a mobile device and evaluating whether the received data is safe or malicious by comparing the received information against known good data and bad known data stored in the server's memory as claimed therein is not present in the invention of Groups I.

Groups I and II lack unity of invention because even though the inventions of these groups require the technical feature of evaluating whether information is good data or bad data by comparison with data stored in a database, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2007/0240218 A1 (TUVELL et al) 11 October 2007 (11.10.2007) paragraph [0103].

Since none of the special technical features of the Group I or II inventions are found in more than one of the inventions, unity of invention is lacking.