



- (51) International Patent Classification:
G06F 21/50 (2013.01) *G06F 21/57* (2013.01)
- (21) International Application Number:
PCT/US2012/062793
- (22) International Filing Date:
31 October 2012 (31.10.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/553,719 31 October 2011 (31.10.2011) US
- (71) Applicant: NEEVO, LLC [US/US]; 7055 Engle Road, Suite 304, Cleveland, Ohio 44130 (US).
- (72) Inventor; and
(71) Applicant : SAUNDERS, Stuart, J. [US/US]; 7055 Engle Road, Suite 304, Cleveland, Ohio 44130 (US).
- (74) Agent: WORGULL, Jason, A.; Renner, Otto, Boisselle & Sklar, LLP, 1621 Euclid Ave., 19th Fl., Cleveland, Ohio 44115 (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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

[Continued on next page]

- (54) Title: SYSTEM AND METHOD FOR APPLICATION SECURITY AND PERFORMANCE ASSESSMENT

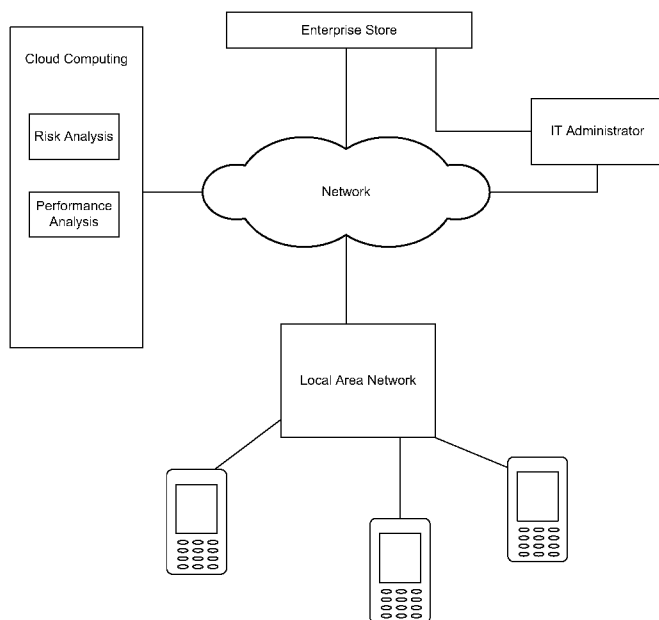


FIG. 4

(57) Abstract: The present application is directed to a system and method for application security and performance assessment. Aspects of the disclosed technology relate to an end-to-end system and method for managing security and privacy risks associated with downloadable applications for devices, as well as for monitoring performance of downloadable applications. The disclosed system and method allows for curation of an application distribution channel in which an enterprise administrator can have top-down and/or bottom-up management of a network of 10 devices. The top-down functionality allows for curation of application based on risk and performance, while the bottom-up functionality allows for real-time removal of harmful items and/or over-the-air healing functionality.



-
- *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))*

SYSTEM AND METHOD FOR APPLICATION SECURITY AND PERFORMANCE ASSESSMENT

Related Application Data

5 This application claims priority of U.S. Provisional Application No. 61/553,719, filed on October 31, 2011, which is incorporated herein by reference in its entirety.

Field of Invention

The present disclosure relates generally to computer security systems and methods, and, more particularly, to system and method for application security and performance assessment.

Background

10 Modern computing devices, such as computers, mobile computing devices, and mobile phones, are capable of downloading and installing a wide variety of software applications. For example, software sources, such as the Android Market, allow users to browse and download applications onto their computing devices. For example, the Android Market, and others like it, allows users to download various
15 applications to their mobile devices, such as their mobile phone. Currently, there are an extremely large number of applications available through sources like the Android Market or the Apple Store.

Different users and computing devices, however, may have different requirements regarding how these applications execute. For example, computing
20 devices may be configured to require that any code executed be authorized by a trusted party. As another example, certain applications may be deemed unsuitable or unsafe for a particular user. Unfortunately, due to the extremely large number of applications, it can be difficult to manage the availability and installation of these applications.

25 Mobile device adoption is poised to overtake conventional computers (laptops, desktops, etc.). Mobile devices may include smart phones, cell phones, personal digital assistants, netbooks, tablet devices, and the like. With the proliferation of mobile devices and their associated operating systems and applications, mobile security poses significant threat to enterprises, service
30 providers, and the like. That is, enterprises are struggling with the consumerization of Information Technology (IT). With the proliferation of mobile devices within the

enterprise, IT administrators can no longer ignore these devices as outside their scope of responsibility. Further, computing power on these devices is now as powerful as laptops. Users may access corporate data and the Internet through wireless networks such as Wi-Fi hotspots or cellular 3G/4G that are not controlled
5 by IT. With many corporate applications being hosted in the cloud, the risk is even higher. Ensuring the security of corporate data is no longer a matter of deploying adequate measures within the organization. It is important that security and policy travel with users wherever they are, on whatever type of device they use. Unlike the personal computer (PC) world that is dominated by a few main operating systems,
10 the number of platforms and device form-factors for mobile devices is much higher, as is their churn rate. IT needs a solution that is easy to deploy, supports multiple mobile platforms and provides consistent user policy enforcement across PCs and mobile devices.

There are challenges that affect IT organizations as the proliferation and
15 adoption of mobile devices increases with enterprises. One challenge is that the line between enterprise and personal usage is getting blurred on mobile devices. These devices run the gamut of applications, from Facebook, YouTube, Pandora, to enterprise apps like email and sales force automation. Since the enterprise typically does not own the device, enforcing policies for acceptable usage or installing
20 application controls like a traditional IT administrator would on a corporate PC is often not viable. There is an increased risk of exposing corporate data on mobile devices since they roam and connect to multiple Wi-Fi and cellular 3G/4G networks. Traditionally, web security protections have been enforced either by way of a gateway web proxy at an enterprise's egress to the Internet or via signature-based
25 anti-virus protections installed on the user PC. With mobile devices, there is no obvious point of enforcement like an enterprise proxy. To complicate matters further, enterprise data is rapidly migrating to the cloud. As a result, an employee's mobile web transactions may never hit the enterprise network while accessing critical cloud-hosted data.

30 Another challenge is that security apps for mobile devices are expensive to

develop and often ineffective. Unlike the PC world, which is dominated by Microsoft, there are several different mobile operating systems--Apple iOS, Android, Windows Mobile, Blackberry, Symbian, etc. Each platform has its own software development environment and a security vendor developing mobile security applications will have to replicate the effort across various platforms. Further, some platforms such as Apple iOS do not allow traditional anti-virus applications on their platform. Loading third party applications, not approved by the platform vendor may lead to violation of contract and may require "jailbreaking" the device--definitely not an enterprise option. Even if security applications are allowed, they are a headache to deploy, require constant updates, and are easy to circumvent--the user can simply uninstall them if they dislike it. Worst of all, they impact device performance and degrade user experience by stretching the already limited processor and memory resources on the mobile device.

With the advent of mobile devices, there has been an explosion of custom built applications that users can download from various mobile markets such as the Apple App Store and the Android Market. The Apple App Store has over 250,000 apps and has crossed the 10 billion download mark. The Android Market is in a similar position. As such, mobile platforms are even more desirable targets for web based exploits given that the devices are always accessible and online and thus more likely to be impacted by a short lived attack.

Summary of Invention

Aspects of the disclosed technology relate to an end-to-end system and method for managing security and privacy risks associated with downloadable applications for devices, as well as for monitoring performance of downloadable applications. The disclosed system and method allows for curation of an application distribution channel in which an enterprise administrator can have top-down and/or bottom-up management of a network of devices. The top-down functionality allows for curation of application based on risk and performance, while the bottom-up

functionality allows for real-time removal of harmful items and/or over-the-air healing functionality.

One aspect of the disclosed technology relates to a method of assessing risk
5 associated with a downloadable application for a mobile device that includes
determining a security risk score associated with the downloadable application; and
determining a privacy risk score associated with the downloadable application.

According to one feature, the method includes determining a composite risk
score based on the determined security risk score and the determined privacy risk
10 score.

According to one feature, determining a security risk score includes defining
a plurality of customizable rules for determining the security risk score.

According to one feature, determining a security risk score includes applying
the plurality of customizable rules to the downloadable application.

15 According to one feature, determining a privacy risk score includes defining a
plurality of customizable rules for determining the privacy risk score.

According to one feature, determining a privacy risk score includes applying
the plurality of customizable rules to the downloadable application.

According to one feature, determining a security risk score includes: mining
20 the downloadable application for code, assets, patterns and/or signatures; and
applying a plurality of customized rules to the mined code, assets, patterns and/or
signatures.

According to one feature, determining a privacy risk score includes: mining
the downloadable application for code, assets, patterns and/or signatures; and
25 applying a plurality of customized rules to the mined code, assets, patterns and/or
signatures.

According to one feature, the method includes comparing the security risk
score to a predetermined security risk threshold.

According to one feature, the predetermined security risk threshold includes
30 a predetermined security risk score.

According to one feature, the predetermined security risk threshold includes a plurality of policies or rules indicative of an unacceptable security risk.

According to one feature, the method includes comparing the privacy risk score to a predetermine privacy risk threshold.

5 According to one feature, the predetermined privacy risk threshold includes a predetermined privacy risk score.

According to one feature, the predetermined privacy risk threshold, includes a plurality of policies or rules indicative of an unacceptable privacy risk.

10 According to one feature, the method includes comparing the composite risk score to a predetermined risk score.

According to one feature, determining a security risk score includes: performing a static analysis on the downloadable application; and performing an active or runtime analysis on the downloadable application.

15 According to one feature, performing an active or runtime analysis includes: generating simulated user activity involving the downloadable application outside a computing environment on the mobile device; and capturing runtime data related to the simulated user activity involving the downloadable application.

20 According to one feature, determining a privacy risk score includes: performing a static analysis on the downloadable application; and performing an active or runtime analysis on the downloadable application.

According to one feature, performing an active or runtime analysis includes: generating simulated user activity involving the downloadable application outside a computing environment on the mobile device; and capturing runtime data related to the simulated user activity involving the downloadable application.

25 According to one feature, the method includes determining a performance score for the downloadable application.

According to one feature, determining a performance score includes defining a plurality of customizable rules for determining the performance score.

30 According to one feature, determining a performance score includes applying the plurality of customizable rules to the downloadable application.

According to one feature, determining a performance score for the downloadable application includes: generating simulated user activity involving the downloadable application outside a computing environment; and capturing runtime data related to the simulated user activity involving the downloadable application.

5 According to one feature, the downloadable application is pre-installed on the mobile device.

According to another aspect of the disclosed technology, a method of assessing risk associated with a downloadable application includes performing a static analysis of the downloadable application; and performing a runtime analysis
10 of the downloadable application.

According to one feature, performing a static analysis includes receiving one or more facts indicative of security risk; and applying one or more rules to the downloadable application.

15 According to one feature, performing a static analysis includes receiving one or more facts indicative of privacy risk; and applying one or more rules to the downloadable application.

According to one feature, performing a static analysis includes mining the downloadable application for code, assets, patterns and/or signatures; and applying a plurality of customized rules to the mined code, assets, patterns and/or
20 signatures.

According to one feature, performing a runtime analysis includes generating simulated user activity involving the downloadable application outside a computing environment; and capturing runtime data related to the simulated user activity involving the downloadable application.

25

Another aspect of the disclosed technology relates to a method of controlling access to a group of downloadable applications that includes: identifying a security risk threshold and a privacy risk threshold for a downloadable application, the security risk threshold being indicative of a maximum allowable security risk for
30 download of the downloadable application, and the privacy risk threshold being

indicative of a maximum allowable privacy risk for download of the downloadable application; determining a security risk score associated with the downloadable application; determining a privacy risk score associated with the downloadable application; and allowing access to the downloadable application if (i) the security
5 risk score is below the identified security risk threshold and (ii) the privacy risk score is below the identified privacy risk threshold.

Another aspect of the disclosed technology relates to a method of determining whether a downloadable mobile application should be available for download that includes: determining a degree of tolerable risk; identifying a risk
10 score indicative of the determined degree of tolerable risk for the downloadable mobile application, wherein the composite risk score includes a security risk component and a privacy risk component; receiving data indicative of a composite risk score; and making the downloadable application available for download if the received risk score is less than the identified risk score.

15 According to one feature, the method includes: identifying a performance score indicative of a threshold of performance for the downloadable mobile application; receiving data indicative of a performance score; and making the downloadable application available for download if the received performance score is greater than the identified performance score.

20 Another aspect of the disclosed technology includes a method for managing a network of mobile devices that includes determining a degree of tolerable risk associated with a downloadable mobile application; identifying a risk score indicative of the determined degree of tolerable risk associated with downloadable mobile applications, wherein the risk score includes a security risk component and a
25 privacy risk component; receiving data indicative of a risk score; and allowing access to a downloadable mobile application if the received risk score is less than the identified risk score.

According to one feature, the method includes identifying a performance score indicative of a threshold of performance for downloadable mobile applications;
30 receiving data indicative of a performance score; and allowing access to a

downloadable mobile application if the received performance score is greater than the identified performance score.

Another aspect of the disclosed technology relates to a method for managing a network of mobile devices that includes capturing data representative of a
5 download of a mobile application by a mobile device within the network; identifying a risk score indicative of a determined degree of tolerable risk for mobile applications, wherein the risk score includes a security risk component and a privacy risk component; receiving data indicative of a risk score associated with the mobile application downloaded by the mobile device within the network; and
10 removing the mobile application from the mobile device within the network if the received risk score is greater than the identified risk score.

Another aspect of the disclosed technology relates to a method for managing a network of mobile devices that includes capturing data representative of a download of a mobile application by a mobile device within the network; determining
15 whether the downloaded mobile application contains a malicious component; and if the downloaded mobile application contains a malicious component, transmitting code to the mobile device, the transmitted code being operable to remove and/or heal the malicious component.

Another aspect of the disclosed technology relates to a method for managing
20 a network of mobile device that includes capturing data representative of a download of a mobile application by a mobile device within the network; determining whether the downloaded mobile application exhibits acceptable performance; and if the downloaded mobile application does not exhibit acceptable performance, transmitting code to the mobile device, the transmitted code being
25 operable to remove the downloaded mobile application or heal the downloaded mobile application.

Another aspect of the disclosed technology relates to a method for managing a network of mobile devices that includes receiving a risk score threshold indicative of a degree of tolerable risk associated with a downloadable mobile application;
30 wherein the risk score threshold includes a security risk score component and a

privacy risk score component; determining a security risk score associated with the downloadable mobile application; determining a privacy risk score associated with the downloadable mobile application; and allowing access to the downloadable mobile application if the determined risk score is less than the identified risk score threshold.

Another aspect of the disclosed technology relates to a method for managing a network of mobile devices that includes capturing data representative of a download of a mobile application by a mobile device within the network; determining whether the downloaded mobile application has a risk score greater than a predetermined risk score indicative of a degree of tolerable risk associated with a downloadable mobile application; and removing the mobile application from the mobile device within the network if the determined risk score is greater than the predetermined risk score.

Another aspect of the disclosed technology relates to a method of curating a store of downloadable applications for a mobile device that includes identifying a risk score for a downloadable application, the risk score being indicative of a maximum allowable risk for download of the downloadable application; determining a security risk score associated with the downloadable application; determining a privacy risk score associated with the downloadable application; and if the security risk score and the privacy risk score are below the identified risk score, making the downloadable application available for download.

Another aspect of the disclosed technology relates to a method for managing a network of mobile device that includes capturing data representative of a download of a mobile application by a mobile device within the network; monitoring code associated with the mobile application at runtime; determining whether the code has changed at runtime; and if the code has changed at runtime, removing the mobile application from the mobile device within the network.

Another aspect of the disclosed technology relates to a method of curating a store of downloadable applications that includes receiving a risk score threshold indicative of a degree of tolerable risk associated with downloadable applications;

wherein the risk score threshold includes a security risk score threshold and a privacy risk score threshold; and dynamically adjusting access to downloadable applications based on the received risk score threshold.

According to one feature, dynamically adjusting access includes determining
5 a risk score for a given downloadable application; comparing the risk score for the given downloadable application to the received risk score threshold; and if the risk score for the given downloadable application is greater than the received risk score threshold, restricting access to the given downloadable application.

According to one feature, the method includes receiving a performance score
10 threshold indicative of a degree of tolerable performance associated with downloadable applications; and dynamically adjusting access to downloadable applications based on the received performance score threshold.

According to one feature, dynamically adjusting access includes: determining
15 a performance score for a given downloadable application; comparing the performance score for the given downloadable application to the received performance score threshold; and if the performance score for the given downloadable application is less than the received performance score threshold, restricting access to the given downloadable application.

Another aspect of the disclosed technology relates to a method of detecting
20 malicious metamorphic code within a downloadable application for a mobile device that includes downloading the downloadable application onto a cloud computer/processor configured to emulate a mobile device; running the downloadable application on the cloud computer/processor; monitoring patterns in code of the downloadable application during running of the downloadable
25 application; and determining whether patterns in the code of the downloadable application change.

Another aspect of the disclosed technology relates to a method of assessing
performance associated with a downloadable application that includes performing a static analysis of the downloadable application; and performing a runtime analysis
30 of the downloadable application.

Another aspect of the disclosed technology relates to a system for assessing risk associated with a downloadable application for a mobile device that includes a processor configured to: determine a security risk score associated with the downloadable application; and determine a privacy risk score associated with the downloadable application.

These and further features of the present invention will be apparent with reference to the following description and attached drawings. In the description and drawings, particular embodiments of the invention have been disclosed in detail as being indicative of some of the ways in which the principles of the invention may be employed, but it is understood that the invention is not limited correspondingly in scope. Rather, the invention includes all changes, modifications and equivalents coming within the spirit and terms of the claims appended thereto.

Features that are described and/or illustrated with respect to one embodiment may be used in the same way or in a similar way in one or more other embodiments and/or in combination with or instead of the features of the other embodiments.

It should be emphasized that the term “comprises/comprising” when used in this specification is taken to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

Brief Description of the Drawings

Many aspects of the invention can be better understood with reference to the following drawings. The components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present invention. Likewise, elements and features depicted in one drawing may be combined with elements and features depicted in additional drawings. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views.

FIG. 1 is a diagrammatic illustration of one exemplary computing environment in which aspects of the disclosed technology may be implemented;

FIG. 2 is a diagrammatic illustration of another exemplary computing environment in which aspects of the disclosed technology may be implemented;

5 FIG. 3 is a diagrammatic illustration of another exemplary computing environment in which aspects of the disclosed technology may be implemented;

FIG. 4 is a diagrammatic illustration of another exemplary computing environment in which aspects of the disclosed technology may be implemented;

10 FIG. 5 is a diagrammatic illustration of another exemplary computing environment in which aspects of the disclosed technology may be implemented;

FIG. 6 is a flow chart illustrating a method of assessing risk associated with an application in accordance with one aspect of the disclosed technology;

FIG. 7 is a flow chart illustrating a method of assessing risk associated with an application in accordance with one aspect of the disclosed technology;

15 FIG. 8 is a flow chart illustrating a method of assessing risk associated with an application in accordance with one aspect of the disclosed technology;

FIG. 9 is a diagrammatic illustration of a system and method for determining security risk in accordance with one aspect of the disclosed technology;

20 FIG. 10 is a diagrammatic illustration of a system and method for determining privacy risk in accordance with one aspect of the disclosed technology;

FIG. 11 is a diagrammatic illustration of a system and method for determining performance in accordance with one aspect of the disclosed technology;

25 FIG. 12 is a flow chart illustrating a method of controlling access to downloadable applications in accordance with one aspect of the disclosed technology;

FIG. 13 is a diagrammatic illustration of a system and method for determining security risk in accordance with one aspect of the disclosed technology;

FIG. 14 is a diagrammatic illustration of a system and method for determining privacy risk in accordance with one aspect of the disclosed technology;

FIG. 15 is a diagrammatic illustration of a system and method for determining performance in accordance with one aspect of the disclosed technology;

FIG. 16 is a diagrammatic illustration of an exemplary graphical user interface in accordance with one aspect of the disclosed technology; and

5

Detailed Description

To illustrate aspects of the disclosed technology in a clear and concise manner, the drawings may not necessarily be to scale and certain features may be shown in somewhat schematic form.

Aspects of the disclosed technology relate to an end-to-end system and method for managing security and privacy risks associated with downloadable applications for devices, as well as for monitoring performance of downloadable applications. One aspect of the disclosed technology relates to a heuristics engine that mines applications (e.g., downloadable mobile applications) for code, assets, patterns and signatures. The overall analysis can include a static portion and an active or runtime portion. Custom rules can be applied to calculate risk scores for privacy and/or security. In addition, performance scores can be calculated. Based on the outcome of an overall static analysis, applications can be routed through various workflows, both internal and external to the system.

One aspect of the internal workflow allows application to be escalated to a behavioral analysis tool that captures runtime data. This can include low-level operating system hooks, encryption spoofing, custom virtual machines, custom operating system kernels, dynamic class loading, network traffic and modifications to device settings.

As will be described more fully below, aspects of the disclosed technology facilitate curation of an application distribution channel in which an enterprise administrator can have top-down and bottom-up management of a network of devices. The disclosed technology can facilitate management of application

30

inventory for an enterprise network of devices, as well as diagnostic and triage functionality for the enterprise network of devices.

In accordance with one aspect, two lightweight software applications (e.g., thin-clients) can be used with the system. In accordance with one exemplary embodiment, one client is configured to provide engineers or administrators with performance monitoring of applications installed on network device. A second exemplary client allows for real-time removal of malware and over-the-air healing functionality to revert malicious payloads. Compromised devices can be tracked to ensure all devices affected by malicious software are quarantined and healed.

As will be discussed more fully below, in general terms, one aspect of the disclosed technology relates to a system and method for application inventory management. Another aspect of the disclosed technology relates to a system and method for device management. Another aspect of the disclosed technology relates to a runtime profiler system and method. Another aspect of the disclosed technology relates to a research toolset system and method. Another aspect of the disclosed technology relates to an onboard agent and associated method that facilitates real-time malware removal, audit of device settings, over-the-air healing, tracking of compromised devices and/or scanning non-enterprise application installs. Yet another aspect of the disclosed technology relates to a system and method for providing a mobile clearinghouse for application security and performance data.

It will be appreciated that aspects of the disclosed technology can be carried out in a number of exemplary computing environments. For example, FIGS. 1-5 illustrate several exemplary computing environments for carrying out aspects of the disclosed technology. One example of an environment suitable for practicing various embodiments of the disclosed technology is provided in FIG. 1. As shown, the system may include an application database, such as a mobile application store through which mobile applications may be downloaded or otherwise transferred to one or more mobile devices.

The application database or store may be configured to include an enterprise

store. The enterprise store functionality may be implemented through one or more enterprise management tools. For example, the Cisco AppHQ manager may be employed for providing a convenient store front experience for mobile devices within an enterprise network. For example, in the case of the Cisco AppHQ store, enterprises that deploy Cisco devices can have the ability to create and manage a secure, customized view of applications in Cisco AppHQ. In addition, Cisco AppHQ enables enterprise IT managers to effectively control the purchase, licensing, distribution and management of approved applications to and users. As is discussed more fully below, this functionality is enhanced by way of the various aspects of the disclosed technology. As shown, the enterprise store provides for control by, monitoring by and communication with an IT administrator or IT manager. Various mobile devices may communicate with the enterprise store through any suitable network, such as the Internet or any suitable wide area network. It will be appreciated that aspects of the disclosed technology are not limited to implementation using Cisco AppHQ. Rather, any suitable enterprise platform may be employed without departing from the scope of the disclosed technology.

FIG. 2 illustrates another exemplary computing environment in which mobile devices associated with an enterprise may communicate directly with an application store outside of the realm of an enterprise store. It will be appreciated that aspects of the disclosed technology provide for management of such a network mobile devices by providing bottom-up functionality for applications downloaded outside of the enterprise environment.

FIG. 3 shows another exemplary computing environment in which a plurality of mobile devices may access public networks and websites, such as an application store, through a security system, e.g., a cloud-based security system through which an IT administrator or manager has access to and input on mobile device operations, such as downloading applications and running applications.

Turning now to FIG. 4, another exemplary computing environment in which aspects of the disclosed technology may be carried out is provided. In the

illustrated exemplary computing environment, a variety of mobile devices may be in communication within a local area network and/or a wide area network through which applications may be downloaded from, for example, an enterprise store.

Alternatively, various mobile device may download application outside of the enterprise environment. Various aspects of the security analysis, risk analysis, and performance analysis may be carried out, for example, in a cloud computing environment. As shown, an IT administrator or manager will have access to the enterprise store as well as risk and/or performance data or information generated through the methods described more fully. For example, the IT administrator can set various risk and/or performance thresholds to provide dynamic filtering of available applications within the enterprise store. Alternatively, the IT administrator may monitor already-installed applications using similar risk and/or performance thresholds. This monitoring can be complemented with real-time removal of malware, as well as over-the-air healing functionality.

FIG. 5 is a simplified computing environment in which an IT administrator may have access to application inventory management information and services as well as device management, diagnostic and triage information and services, for example, hosted on a cloud. These features can provide an IT manager with top-down and bottom-up network management functionality.

While for purposes of simplicity of explanation, various flow charts or diagrams include a series of steps or functional blocks that represent one or more aspects of the relevant operation of the system and method, it is to be understood and appreciated that aspects of the disclosed technology are not limited to the order of steps or functional blocks, as some steps or functional blocks may, in accordance with aspects of the disclosed technology, occur in different orders and/or concurrently with other steps or functional blocks from that shown and described herein. Moreover, not all illustrated steps or functional blocks of aspects of relevant operation may be required to implement a methodology in accordance with an aspect of the disclosed technology. Furthermore, additional steps or functional blocks of aspects of relevant operation may be added without departing from the

scope of the disclosed technology.

Turning now to FIG. 6, a method of assessing risk associated with an application, for example, a downloadable application accessible through an application store or a pre-installed application is provided. The method begins at a first step where a security risk score is determined for a given application. It will be appreciated that determining a security risk score can be implemented in a variety of ways without departing from the scope of the disclosed technology. For example, determining security risk score can include defining a plurality of customizable rules and/or facts for determining the security risk score and applying the plurality of customizable rules and/or facts to the application. Further, determining a security risk score can include mining the downloadable application for code, assets, patterns and/or signatures and applying a plurality or customizable rules or facts to the mind.

In accordance with another exemplary embodiment, a security risk score can be determined or otherwise computed based on a security analysis done for the application, application permissions which determine what the application is capable of accessing, reputation of the vendor that created the application, feedback from users, real-time analysis of application behavior in the cloud, or combinations of the above.

Next, a privacy risk score is determined for the application. In accordance with one embodiment, determining a privacy risk score can include defining a plurality of customizable rules or facts for determining the privacy risk score and applying the plurality of customizable rules or facts to the application. Determining a privacy risk score can include mining the application for code, assets, patterns and/or signatures and applying a plurality of customized rules to the mind code, assets, patterns and/or signatures.

In another exemplary embodiment, privacy risk score may be based on a privacy analysis performed for the application, feedback from users of the application around security, real-time analysis of application behavior in the cloud or combinations of the above. As will be discussed more fully below, the determination

of the security risk score and/or a privacy risk score will allow for dynamic filtering of application inventory. For example, if a particular application is requested by a mobile device, access to the application may be granted or denied depending on whether the requested application meets a minimum threshold for security and/or privacy as set forth by an IT administrator or manager.

In accordance with another exemplary embodiment, a composite risk score can be calculated based on the determined security risk score and/or the determined privacy risk score.

In accordance with another embodiment (FIG. 7), applications may be examined and assigned a performance score, which may be a numerical score or may be a pass/no pass score indicative of whether the application meets minimum performance requirements or standards for the given enterprise rules and/or policies.

In accordance with one embodiment (FIG. 8 and FIG. 9), determining a security risk score can include performing a static analysis on the application and/or performing an active or runtime analysis on the application. In accordance with one embodiment, if the application passes the static analysis, then an active or run time analysis may be performed. However, if the application does not pass the static analysis, there is no need to perform an active or run time analysis of the application. Likewise, determining a privacy risk score can include performing a static analysis on the application and/or performing an active or runtime analysis on the application.

In accordance with one embodiment, performing an active or runtime analysis can include generating simulated user activity involving the application outside the computing environment on the mobile device and capturing runtime data related to the simulated user activity involving the downloadable application. For example, an application may be downloaded onto a suitable cloud server or cloud processor which simulates a download on a mobile device. The cloud server or cloud processor may engage in normal runtime use of the application, where runtime data related to the simulated user activity is captured and used to determine

whether the application presents any security risk or privacy risk.

In accordance with another exemplary embodiment, a method of assessing risk includes performing a static analysis of the application, for example, a downloadable application or a pre-installed application. In accordance with one
5 embodiment, performing a static analysis can include receiving one or more facts indicative of security risk, as well as receiving one or more facts indicative of privacy risks. The method of performing a static analysis can include applying one or more rules to the downloadable application based on the received facts indicative of security risks as well as applying one or more rules to the application based on the
10 one or more facts indicative of privacy risk.

Another aspect of the disclosed technology relates to a method of controlling access to a group of downloadable applications (FIG. 12). The method can include receiving or otherwise identifying a risk threshold. As is discussed above, a risk threshold can be related to a given security risk threshold or score and/or a given
15 privacy risk threshold or score. A risk score can be determined for a given application, including determining a security risk score for the application and/or a privacy risk score for the application. If the determined risk score exceeds the received risk threshold, access to the application can be denied and/or the application can be removed from the available inventory in the given enterprise
20 store.

In accordance with another embodiment, application performance can be viewed in determining access to a given application. For example, if a risk threshold has been identified and risk has been determined for a given application, where the risk score does not exceed the received risk threshold, performance criteria can be
25 determined or otherwise received. If the application satisfies the performance criteria and/or receives a sufficiently high performance score, the application can be made available to download. Alternatively, if the application does not satisfy the performance criteria and/or receives a sufficiently low performance score, access to the application can be blocked and/or the application can be removed from the
30 available inventory, for example, in the enterprise store.

Another aspect of the disclosed technology relates to a method of managing a network of mobile devices. The method includes capturing data representative of a download of a mobile application by a mobile device within the network. The method further includes identifying a risk threshold indicative of a determined
5 degree of tolerable risk, wherein a risk threshold includes a security risk component and a privacy risk component. Data indicative of a security risk score is received and data indicative of a privacy risk score is received. The mobile application can be removed from the mobile device within the network if the received security risk score and/or privacy risk score is greater than the identified risk threshold.

10 In accordance with another embodiment, determining a security risk score, a privacy risk score and/or a performance score can be achieved using a static or passive analysis and an active or runtime analysis, together with third party data. (See, e.g., FIGS. 13-15). It will be appreciated that numerous third-party databases can be used without departing from the scope of the present invention. For
15 example, aspects of the disclosed technology may be used in conjunction with a third-party analysis or data, (e.g., known vulnerabilities and exposures or other known security risk data, privacy risk data and/or performance data). For example, to Common Vulnerabilities and Exposures (CVE) database can be accessed and used in connection with aspects of the disclosed technology.

20 Below are the CVE Initiative's definitions of the terms "Vulnerability" and "Exposure":

Vulnerability

25 An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes entirely "open" security
30 policies in which all users are trusted, or where there is no consideration of risk to

NEVOP0101US

the system).

For CVE, a vulnerability is a state in a computing system (or set of systems) that either:

5

- allows an attacker to execute commands as another user
- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity

10

- allows an attacker to conduct a denial of service

Examples of vulnerabilities include:

15

- phf (remote command execution as user "nobody")
- rpc.ttdbserverd (remote command execution as root)
- world-writeable password file (modification of system-critical data)
- default password (remote command execution or other access)
- denial of service problems that allow an attacker to cause a Blue Screen of Death
- smurf (denial of service by flooding a network)

20

Review vulnerabilities on the Common Vulnerabilities and Exposures (CVE) List.

Exposure

25

An information security "exposure" is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

30

CVE considers a configuration issue or a mistake an exposure if it does not directly allow compromise but could be an important component of a successful attack, and

is a violation of a reasonable security policy.

An "exposure" describes a state in a computing system (or set of systems) that is not a vulnerability, but either:

5

- allows an attacker to conduct information gathering activities
 - allows an attacker to hide activities
 - includes a capability that behaves as expected, but can be easily compromised
 - is a primary point of entry that an attacker may attempt to use to gain access to the
- 10 system or data

- is considered a problem according to some reasonable security policy

Examples of exposures include:

15

- running services such as finger (useful for information gathering, though it works as advertised)
 - inappropriate settings for Windows NT auditing policies (where "inappropriate" is enterprise-specific)
 - running services that are common attack points (e.g., HTTP, FTP, or SMTP)
 - use of applications or services that can be successfully attacked by brute force methods (e.g., use of trivially broken encryption, or a small key space)
- 20

25

In accordance with one exemplary embodiment, a mobile clearinghouse for data can be established using the risk and performance analysis described above, together with accessing and processing information within third-party databases, such as the above-described CVE database.

30

While aspects of the disclosed technology have been described in connection with controlling access to downloadable applications, it will be appreciated that aspects of the disclosed technology may also be applied to a

method of controlling access to a distribution channel or knowledge based in which one or more applications may have already been downloaded by a mobile device within the network. In accordance with this embodiment, a security risk analysis and a privacy risk analysis may be performed alone or together with a performance analysis. If it is found that the previously downloaded or otherwise pre-installed application violates a given risk threshold (whether it be security risk threshold or privacy risk threshold) or violates specific performance metrics, proactive action can be taken to remedy the situation. Such action can include, but is not limited to, removing the application and/or any malware associated with the application, as well as over-the-air-healing functionality to revert any malicious payloads. In this manner, compromised devices can be tracked to ensure that all devices affected by malicious software are quarantined and healed.

As is discussed above, the various embodiments of the disclosed system and method provide an IT administrator with information and/or functionality to manage security and privacy risks and performance for mobile devices within an enterprise. One aspect of the disclosed technology includes a user interface configured to receive input from an IT administrator. FIG. 16 shows a very simplified graphical user interface in which an IT administrator can adjust various risk and performance thresholds. For example, the exemplary graphical user interface includes a plurality of user-selectable sliders representative of a desired threshold for privacy risk, security risk and performance. Through this graphical user interface an IT administrator can adjust threshold values for privacy risk threshold, security risk threshold and/or performance threshold and receive dynamic feedback as to the effects on application availability within an enterprise store.

Alternatively, this type of feedback can be provided with respect to already-installed applications on mobile devices within the network.

While the exemplary graphical user interface includes virtual sliders, it will be appreciated that any user-selectable interface can be employed without departing from the scope of the disclosed technology.

Also, while aspects of the privacy risk score, security risk score and/or

performance risk score are described or alluded to in numerical terms, it will be appreciated that qualitative thresholds can also be employed without departing from the scope of the disclosed technology.

5 It will be appreciated that above-described application security system and method finds broad application in connection with managing security and privacy risks and performance for mobile devices within a network.

10 Although the invention has been shown and described with respect to a certain embodiment or embodiments, it is obvious that equivalent alterations and modifications will occur to others skilled in the art upon the reading and understanding of this specification and the annexed drawings. In particular regard to the various functions performed by the above described elements (components, assemblies, devices, compositions, etc.), the terms (including a reference to a
15 "means") used to describe such elements are intended to correspond, unless otherwise indicated, to any element which performs the specified function of the described element (i.e., that is functionally equivalent), even though not structurally equivalent to the disclosed structure which performs the function in the herein illustrated exemplary embodiment or embodiments of the invention. In addition,
20 while a particular feature of the invention may have been described above with respect to only one or more of several illustrated embodiments, such feature may be combined with one or more other features of the other embodiments, as may be desired and advantageous for any given or particular application.

Claims

What is claimed is:

1. A method of assessing risk associated with a downloadable application
5 for a mobile device, the method comprising:
determining a security risk score associated with the downloadable
application; and
determining a privacy risk score associated with the downloadable
application.
10
2. The method of claim 1, further comprising:
determining a composite risk score based on the determined security risk
score and the determined privacy risk score.
- 15 3. The method of claim 1 or claim 2, wherein determining a security risk
score includes defining a plurality of customizable rules for determining the security
risk score.
4. The method of any of claims 1-3, wherein determining a security risk
20 score includes applying the plurality of customizable rules to the downloadable
application.
5. The method any of claims 1-4, wherein determining a privacy risk
score includes defining a plurality of customizable rules for determining the privacy
25 risk score.
6. The method of claim 5, wherein determining a privacy risk score
includes applying the plurality of customizable rules to the downloadable application.
- 30 7. The method of any of claims 1-6, wherein determining a security risk
score includes:

mining the downloadable application for code, assets, patterns and/or signatures; and

applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

5

8. The method of any of claims 1-7, wherein determining a privacy risk score includes:

mining the downloadable application for code, assets, patterns and/or signatures; and

10 applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

9. The method of any of claims 1-8, further comprising:

comparing the security risk score to a predetermined security risk threshold.

15

10. The method of claim 9, wherein the predetermined security risk threshold includes a predetermined security risk score.

11. The method of claim 9, wherein the predetermined security risk threshold, includes a plurality of policies or rules indicative of an unacceptable security risk.

20

12. The method of any of claims 1-11, further comprising:

comparing the privacy risk score to a predetermine privacy risk threshold.

25

13. The method of claim 12, wherein the predetermined privacy risk threshold includes a predetermined privacy risk score.

14. The method of claim 12, wherein the predetermined privacy risk threshold, includes a plurality of policies or rules indicative of an unacceptable privacy risk.

30

15. The method of any of claims 2-14, further comprising:
comparing the composite risk score to a predetermined risk score.

5 16. The method of any of claims 1-15, wherein determining a security risk
score includes:

performing a static analysis on the downloadable application; and
performing an active or runtime analysis on the downloadable application.

10 17. The method of claim 16, wherein performing an active or runtime
analysis includes:

generating simulated user activity involving the downloadable application
outside a computing environment on the mobile device; and

15 capturing runtime data related to the simulated user activity involving the
downloadable application.

18. The method of any of claims 1-17, wherein determining a privacy risk
score includes:

20 performing a static analysis on the downloadable application; and
performing an active or runtime analysis on the downloadable application.

19. The method of claim 18, wherein performing an active or runtime
analysis includes:

25 generating simulated user activity involving the downloadable application
outside a computing environment on the mobile device; and

capturing runtime data related to the simulated user activity involving the
downloadable application.

20. The method of any of claims 1-19, further comprising:
30 determining a performance score for the downloadable application.

21. The method of any of claims 1-20, wherein determining a performance score includes defining a plurality of customizable rules for determining the performance score.

5 22. The method of claim 21, wherein determining a performance score includes applying the plurality of customizable rules to the downloadable application.

23. The method of claim 20, wherein determining a performance score for the downloadable application includes:

10 generating simulated user activity involving the downloadable application outside a computing environment; and
 capturing runtime data related to the simulated user activity involving the downloadable application.

15 24. The method of any of claims 1-23, wherein the downloadable application is pre-installed on the mobile device.

25. A method of assessing risk associated with a downloadable application, the method comprising

20 performing a static analysis of the downloadable application; and
 performing a runtime analysis of the downloadable application.

26. The method of claim 25, wherein performing a static analysis includes: receiving one or more facts indicative of security risk; and

25 applying one or more rules to the downloadable application.

27. The method of claim 25 or claim 26, wherein performing a static analysis includes:

 receiving one or more facts indicative of privacy risk; and
30 applying one or more rules to the downloadable application.

28. The method of any of claims 25-27, wherein performing a static analysis includes:

mining the downloadable application for code, assets, patterns and/or signatures; and

5 applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

29. The method of any of claims 25-28, wherein performing a runtime analysis includes:

10 generating simulated user activity involving the downloadable application outside a computing environment; and

capturing runtime data related to the simulated user activity involving the downloadable application.

15 30. A method of controlling access to a group of downloadable applications, the method including:

identifying a security risk threshold and a privacy risk threshold for a downloadable application, the security risk threshold being indicative of a maximum allowable security risk for download of the downloadable application, and the privacy risk threshold being indicative of a maximum allowable privacy risk for download of the downloadable application;

20 determining a security risk score associated with the downloadable application;

determining a privacy risk score associated with the downloadable application; and

25 allowing access to the downloadable application if (i) the security risk score is below the identified security risk threshold and (ii) the privacy risk score is below the identified privacy risk threshold.

30 31. The method of claim 30, wherein determining a security risk score includes defining a plurality of customizable rules for determining the security risk

score.

32. The method of claim 31, wherein determining a security risk score includes applying the plurality of customizable rules to the downloadable application.

5

33. The method of any of claims 30-32, wherein determining a privacy risk score includes defining a plurality of customizable rules for determining the privacy risk score.

10

34. The method of claim 33, wherein determining a privacy risk score includes applying the plurality of customizable rules to the downloadable application.

35. The method of any of claims 30-34, wherein determining a security risk score includes:

15

mining the downloadable application for code, assets, patterns and/or signatures; and

applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

20

36. The method of any of claims 30-35, wherein determining a privacy risk score includes:

mining the downloadable application for code, assets, patterns and/or signatures; and

25

applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

37. The method of any of claims 30-36, further comprising:
comparing the security risk score to the predetermined security risk threshold.

30

38. The method of claim 37, wherein the predetermined security risk threshold includes a predetermined security risk score.

39. The method of claim 37, wherein the predetermined security risk threshold, includes a plurality of policies or rules indicative of an unacceptable security risk.

5

40. The method of any of claims 30-39, further comprising:
comparing the privacy risk score to a predetermine privacy risk threshold.

41. The method of claim 40, wherein the predetermined privacy risk
10 threshold includes a predetermined privacy risk score.

42. The method of claim 40, wherein the predetermined privacy risk threshold, includes a plurality of policies or rules indicative of an unacceptable privacy risk.

15

43. The method of any of claims 30-42, wherein determining a security risk score includes:

performing a static analysis on the downloadable application; and
performing a runtime analysis on the downloadable application.

20

44. The method of claim 43, wherein performing a runtime analysis includes:

generating simulated user activity involving the downloadable application outside a computing environment; and

25 capturing runtime data related to the simulated user activity involving the downloadable application.

45. The method of any of claims 30-44, wherein determining a privacy risk score includes:

30 performing a static analysis on the downloadable application; and
performing a runtime analysis on the downloadable application.

46. The method of claim 45, wherein performing a runtime analysis includes:

generating simulated user activity involving the downloadable application
5 outside a computing environment; and
capturing runtime data related to the simulated user activity involving the downloadable application.

47. The method of any of claims 30-46, the method further comprising:
10 identifying a performance threshold for the downloadable application;
determining a performance score associated with the downloadable application; and

allowing access to the downloadable application if the performance score is above the identified performance threshold.

48. The method of claim 47, wherein determining a performance score includes:

generating simulated user activity involving the downloadable application
outside a computing environment; and

20 capturing runtime data related to the simulated user activity involving the downloadable application.

49. A method of determining whether a downloadable mobile application should be available for download, the method comprising:

25 determining a degree of tolerable risk;
identifying a risk score indicative of the determined degree of tolerable risk for the downloadable mobile application, wherein the composite risk score includes a security risk component and a privacy risk component;

receiving data indicative of a composite risk score; and

30 making the downloadable application available for download if the received risk score is less than the identified risk score.

50. The method of claim 49, further comprising:
identifying a performance score indicative of a threshold of performance for
the downloadable mobile application;

5 receiving data indicative of a performance score; and
making the downloadable application available for download if the received
performance score is greater than the identified performance score.

51. A method for managing a network of mobile devices, the method
10 comprising:
determining a degree of tolerable risk associated with a downloadable mobile
application;

identifying a risk score indicative of the determined degree of tolerable risk
associated with downloadable mobile applications, wherein the risk score includes a
15 security risk component and a privacy risk component;

receiving data indicative of a risk score; and
allowing access to a downloadable mobile application if the received risk
score is less than the identified risk score.

20 52. The method of claim 51, further comprising:
identifying a performance score indicative of a threshold of performance for
downloadable mobile applications;

receiving data indicative of a performance score; and
allowing access to a downloadable mobile application if the received
25 performance score is greater than the identified performance score.

53. A method for managing a network of mobile devices, the method
comprising:

capturing data representative of a download of a mobile application by a
30 mobile device within the network;

identifying a composite risk score indicative of a determined degree of

tolerable risk, wherein the composite risk score includes a security risk component and a privacy risk component;

receiving data indicative of a composite risk score associated with the mobile application downloaded by the mobile device within the network; and

5 removing the mobile application from the mobile device within the network if the received composite risk score is greater than the identified composite risk score.

54. The method of claim 53, further comprising:

10 identifying a performance score indicative of a threshold of performance for mobile applications;

receiving data indicative of a performance score associated with the mobile application downloaded by the mobile device within the network; and

removing the mobile application from the mobile device within the network if the received performance score is greater than the identified performance score.

15

55. A method for managing a network of mobile devices, the method comprising:

capturing data representative of a download of a mobile application by a mobile device within the network;

20 determining whether the downloaded mobile application contains a malicious component; and

if the downloaded mobile application contains a malicious component, transmitting code to the mobile device, the transmitted code being operable to remove and/or heal the malicious component.

25

56. A method for managing a network of mobile devices, the method comprising:

receiving a composite risk score threshold indicative of a degree of tolerable risk associated with a downloadable mobile application; wherein the composite risk score includes a security risk score and a privacy risk score;

30

determining a security risk score associated with the downloadable mobile

application;

determining a privacy risk score associated with the downloadable mobile application;

5 determining a composite risk score based on the determined security risk score and the determined privacy risk score; and

allowing access to the downloadable mobile application if the determined composite risk score is less than the identified composite risk score.

10 57. A method for managing a network of mobile devices, the method comprising:

capturing data representative of a download of a mobile application by a mobile device within the network;

15 determining whether the downloaded mobile application has a composite risk score greater than a predetermined risk score indicative of a degree of tolerable risk associated with a downloadable mobile application; and

removing the mobile application from the mobile device within the network if the determined composite risk score is greater than the predetermined composite risk score.

20 58. The method of claim 57, wherein determining whether the downloaded mobile application has a composite risk score greater than a predetermined risk score includes determining a composite risk score for the downloaded mobile application.

25 59. The method of claim 57 or claim 58, wherein determining a composite risk score includes:

determining a privacy risk score; and
determining a security risk score.

30 60. The method of any of claims 57-59, wherein determining a security risk score includes defining a plurality of customizable rules for determining the security

risk score.

61. The method of any of claims 57-60, wherein determining a security risk score includes applying the plurality of customizable rules to the downloadable application.

62. The method of any of claims 57-61, wherein determining a privacy risk score includes defining a plurality of customizable rules for determining the privacy risk score.

63. The method of any of claims 57-62, wherein determining a privacy risk score includes applying the plurality of customizable rules to the downloadable application.

64. The method of any of claims 57-63, wherein determining a security risk score includes:

mining the downloadable application for code, assets, patterns and/or signatures; and

applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

65. The method of any of claims 57-64, wherein determining a privacy risk score includes:

mining the downloadable application for code, assets, patterns and/or signatures; and

applying a plurality of customized rules to the mined code, assets, patterns and/or signatures.

66. The method of any of claims 57-65, further comprising:

comparing the security risk score to a predetermined security risk score.

67. The method of any of claims 57-66, further comprising:
comparing the privacy risk score to a predetermine privacy risk score.

5 68. The method of any of claims 57-67, further comprising:
comparing the composite risk score to a predetermined risk score.

69. The method of any of claims 57-68, wherein determining a security risk
score includes:
performing a static analysis on the downloadable application; and
10 performing a dynamic analysis on the downloadable application.

70. The method of any of claims 57-69, wherein performing a dynamic
analysis includes:
generating simulated user activity involving the downloadable application
15 outside a computing environment on the mobile device; and
capturing runtime data related to the simulated user activity involving the
downloadable application.

71. The method of any of claims 57-70, wherein determining a privacy risk
20 score includes:
performing a static analysis on the downloadable application; and
performing a dynamic analysis on the downloadable application.

72. The method of any of claims 57-71, wherein performing a dynamic
25 analysis includes:
generating simulated user activity involving the downloadable application
outside a computing environment on the mobile device; and
capturing runtime data related to the simulated user activity involving the
downloadable application.

30 73. The method of any of claims 57-72, further comprising:

determining whether the downloaded mobile application has a performance score greater than a predetermined performance score indicative of a degree of tolerable performance associated with a downloadable mobile application; and

5 removing the mobile application from the mobile device within the network if the determined performance score is less than the predetermined performance score.

74. A method of curating a store of downloadable applications for a mobile device, the method comprising:

10 identifying a composite risk score for a downloadable application, the composite risk score being indicative of a maximum allowable risk for download of the downloadable application;

determining a security risk score associated with the downloadable application;

15 determining a privacy risk score associated with the downloadable application;

determining a composite risk score based on the determined security risk score and the determined privacy risk score; and

20 if the composite risk score is below the identified composite risk score, making the downloadable application available for download.

75. A method for managing a network of mobile devices, the method comprising:

25 capturing data representative of a download of a mobile application by a mobile device within the network;

monitoring code associated with the mobile application at runtime;

determining whether the code has changed at runtime; and

if the code has changed at runtime, removing the mobile application from the mobile device within the network.

30

76. A method of curating a store of downloadable applications, the method

comprising:

receiving a composite risk score threshold indicative of a degree of tolerable risk associated with downloadable applications; wherein the composite risk score includes a security risk score and a privacy risk score; and

5 dynamically adjusting access to downloadable based on the received composite risk score.

77. The method of claim 76, wherein dynamically adjusting access includes:

10 determining a composite risk score for a given downloadable application;
comparing the composite risk score for the given downloadable application to the received composite risk score threshold; and

if the composite risk score for the given downloadable application is greater than the received composite risk score threshold, restricting access to the given
15 downloadable application.

78. The method of claim 76 or claim 77, further comprising:

receiving a performance score threshold indicative of a degree of tolerable performance associated with downloadable applications; and

20 dynamically adjusting access to downloadable applications based on the received performance score threshold.

79. The method of any of claims 76-78, wherein dynamically adjusting access

25 includes:

determining a performance score for a given downloadable application;
comparing the performance score for the given downloadable application to the received performance score threshold; and

if the performance score for the given downloadable application is less than
30 the received performance score threshold, restricting access to the given downloadable application.

80. A method of detecting malicious metamorphic code within a downloadable application for a mobile device, the method comprising:
downloading the downloadable application onto a cloud computer/processor
5 configured to emulate a mobile device;
running the downloadable application on the cloud computer/processor;
monitoring patterns in code of the downloadable application during running of the downloadable application; and
determining whether patterns in the code of the downloadable application
10 change.

81. A method of assessing performance associated with a downloadable application, the method comprising
performing a static analysis of the downloadable application; and
15 performing a dynamic analysis of the downloadable application.

82. The method of claim 81, wherein performing a static analysis includes:
receiving one or more facts indicative of performance; and
applying one or more rules to the downloadable application.

83. The method of claim 81 or claim 82, wherein performing a runtime analysis includes:
generating simulated user activity involving the downloadable application
outside a computing environment; and
25 capturing runtime data related to the simulated user activity involving the downloadable application.

84. A system for assessing risk associated with a downloadable application for a mobile device, the system comprising:
30 a processor configured to:
determine a security risk score associated with the downloadable application;

and

determine a privacy risk score associated with the downloadable application.

1/11

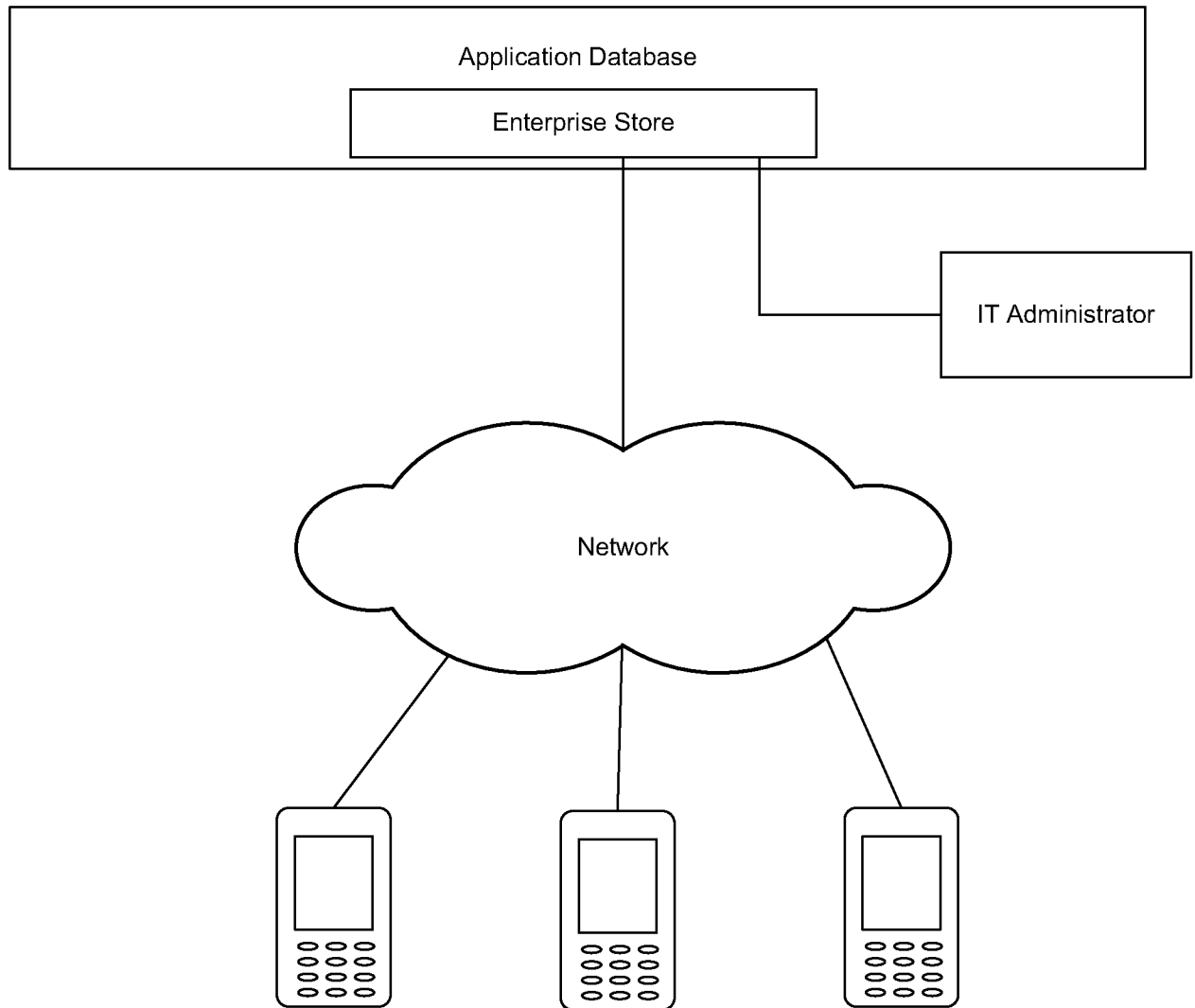


FIG. 1

2/11

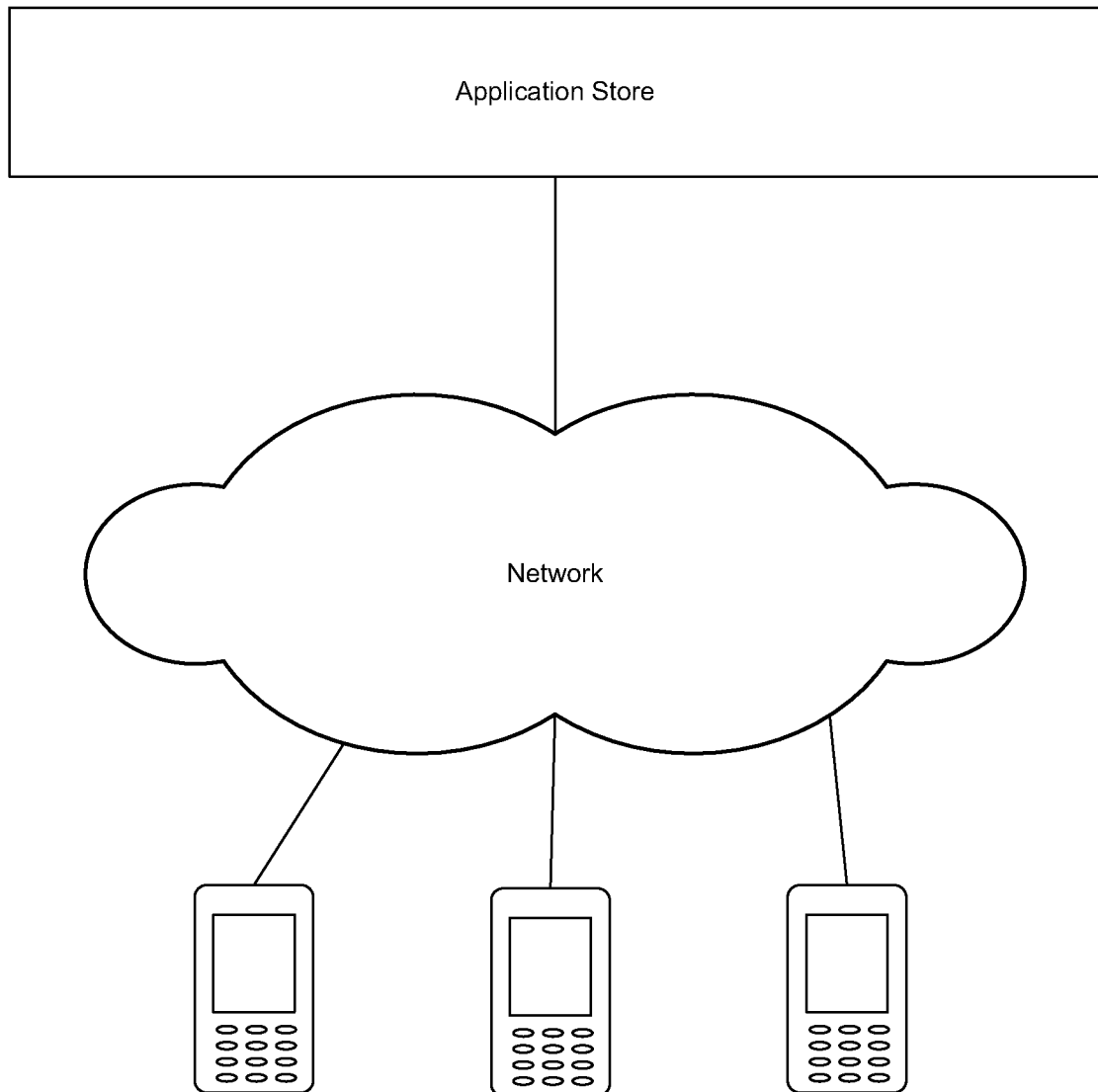


FIG. 2

3/11

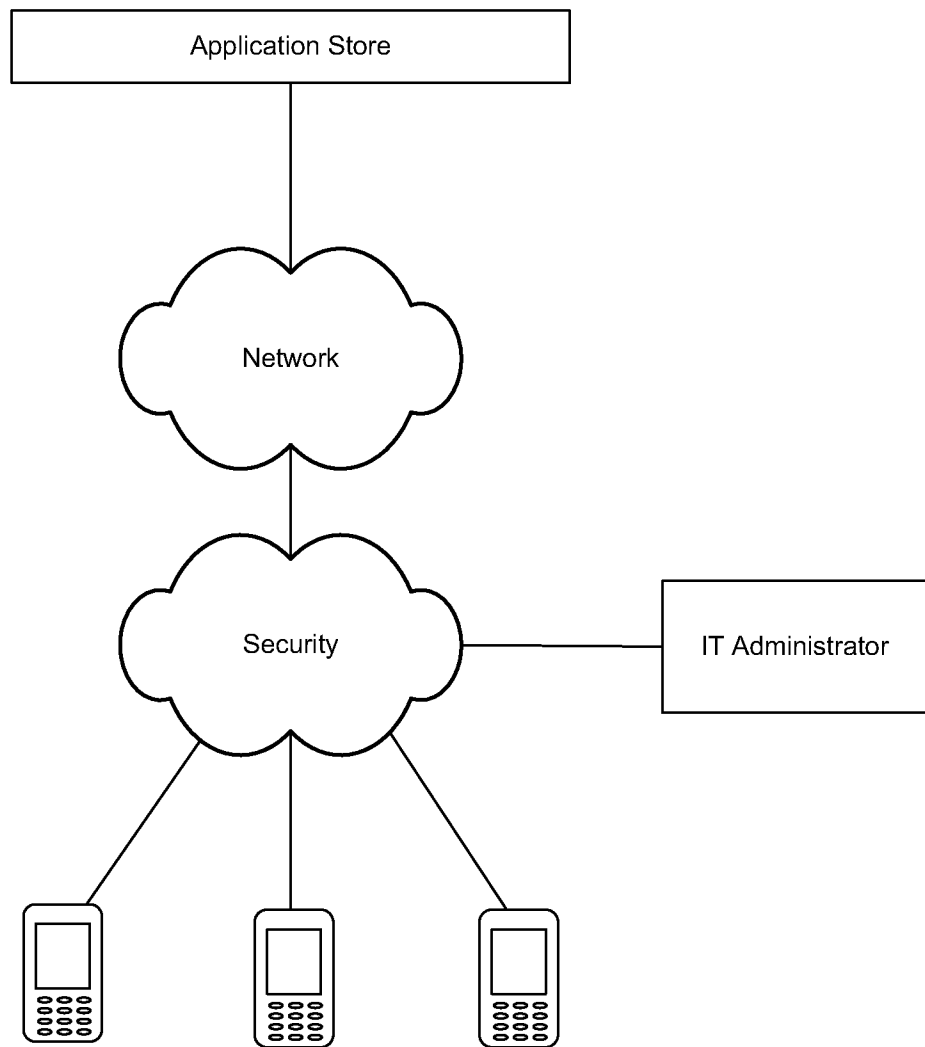
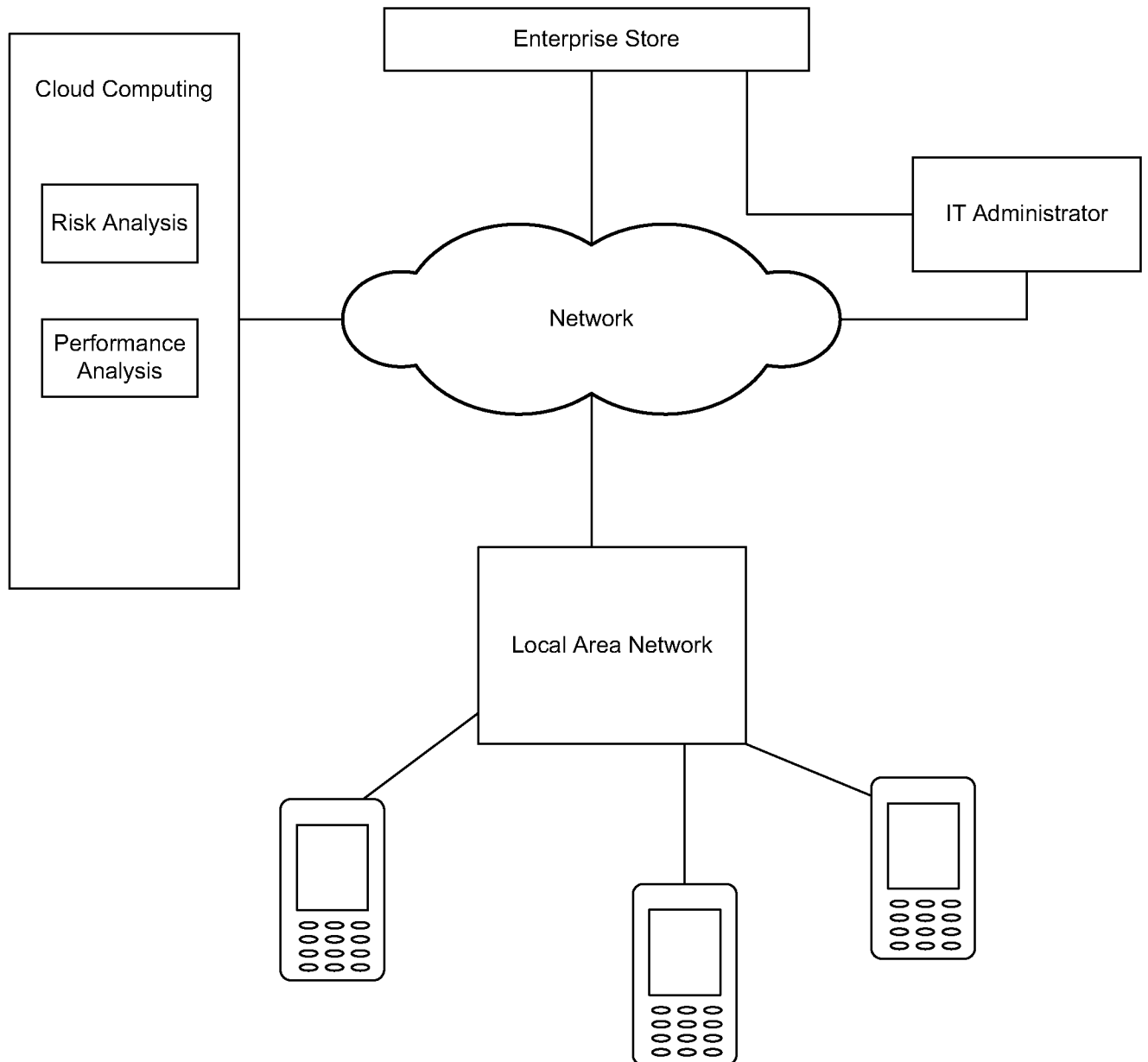
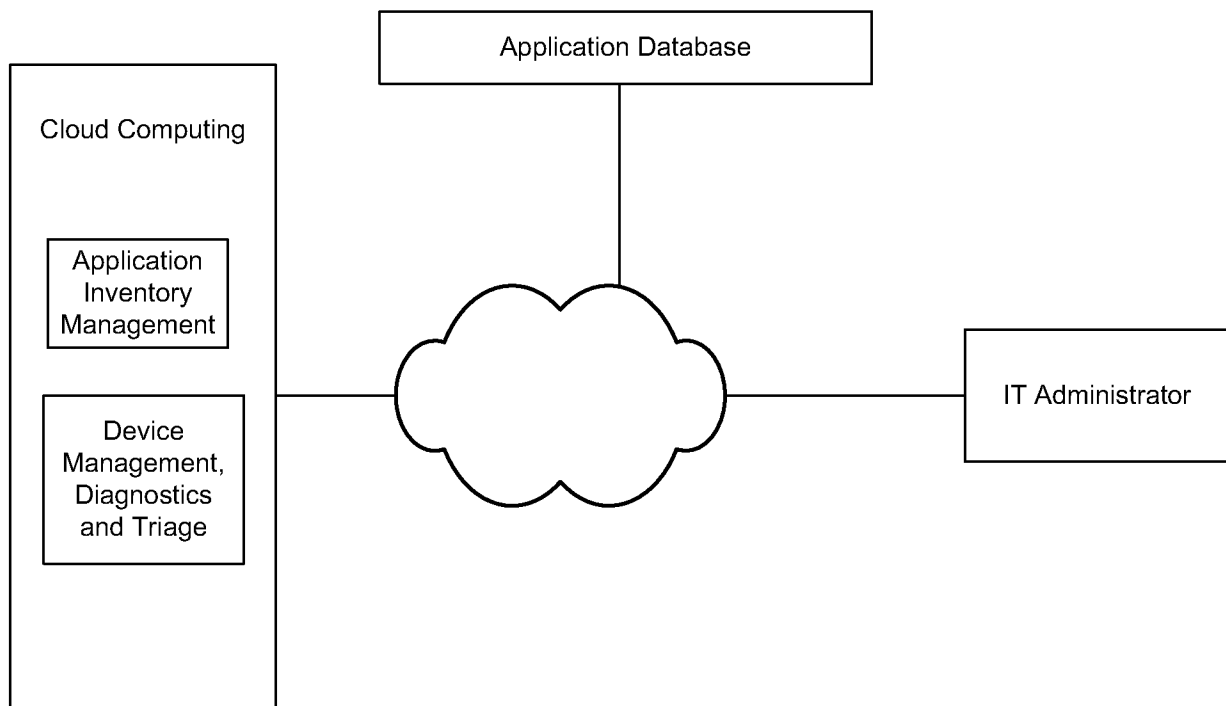


FIG. 3

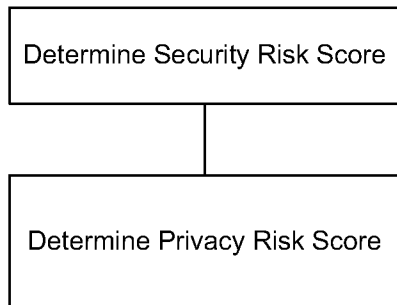
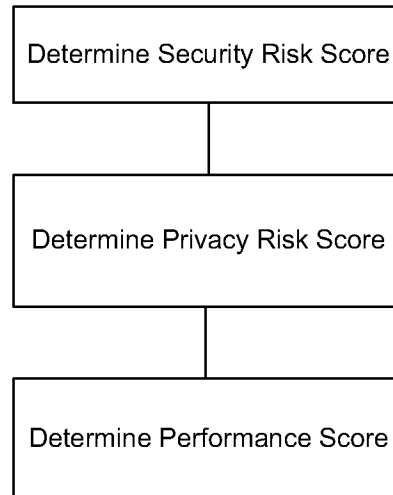
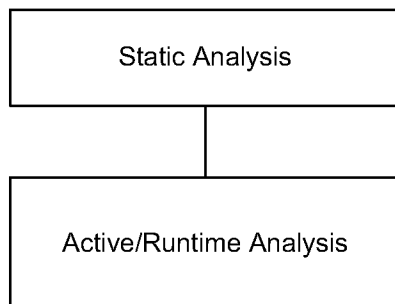
4/11

**FIG. 4**

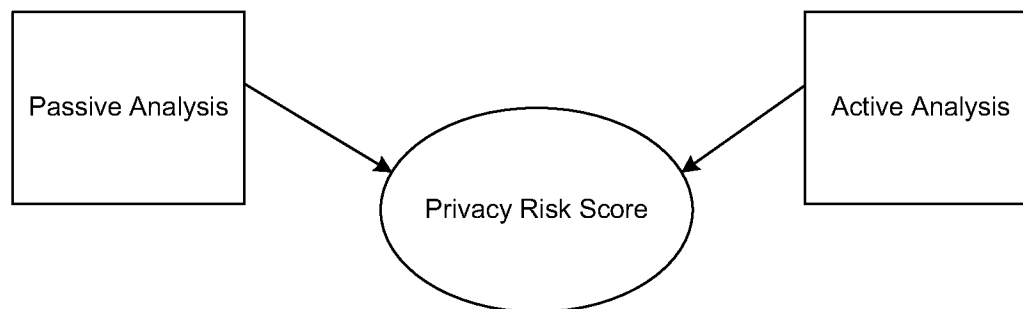
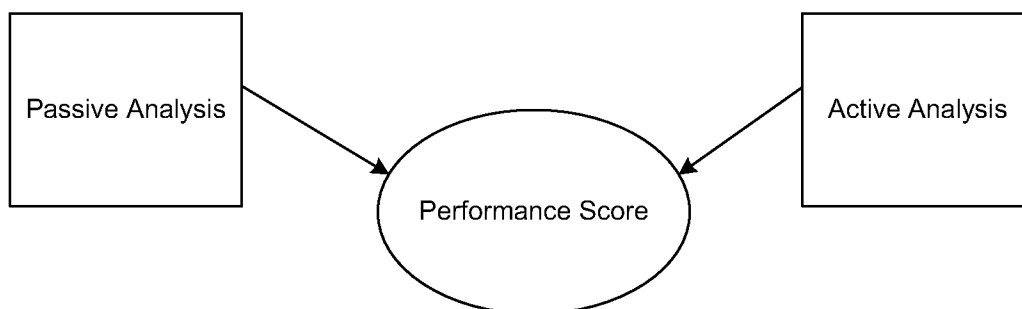
5/11

**FIG. 5**

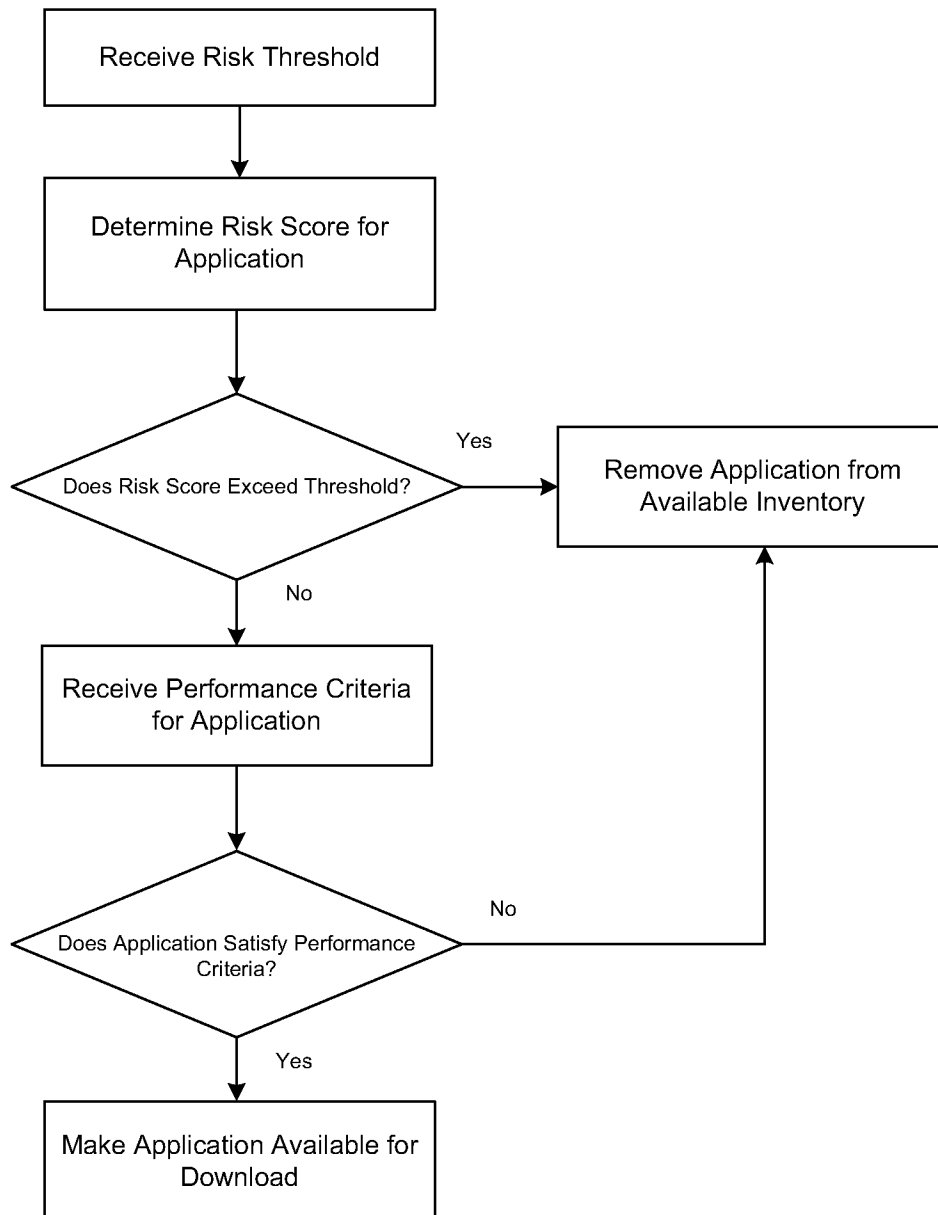
6/11

**FIG. 6****FIG. 7****FIG. 8**

7/11

**FIG. 9****FIG. 10****FIG. 11**

8/11

**FIG. 12**

9/11

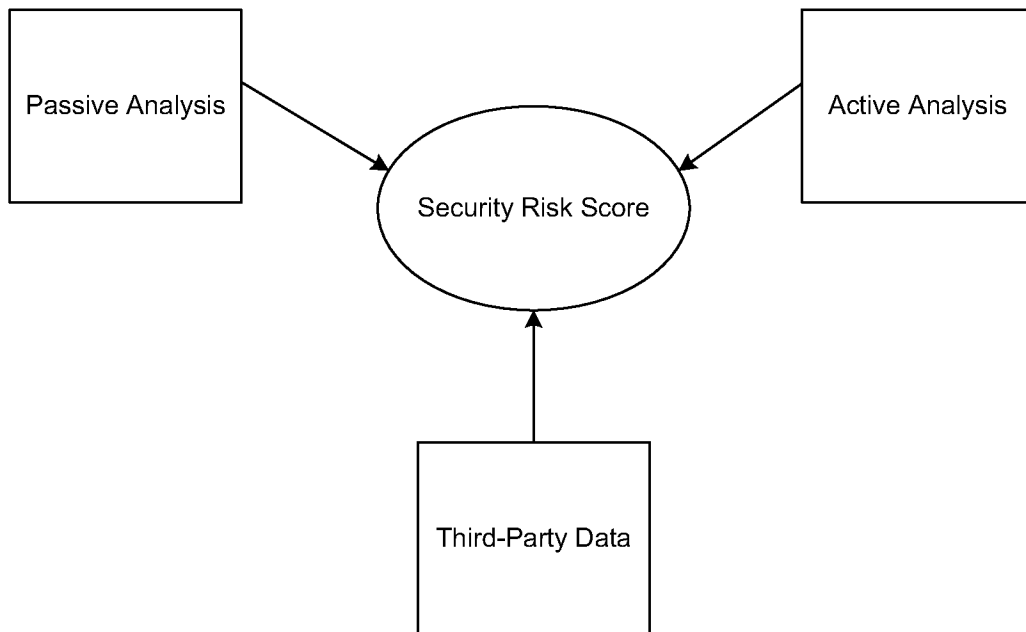


FIG. 13

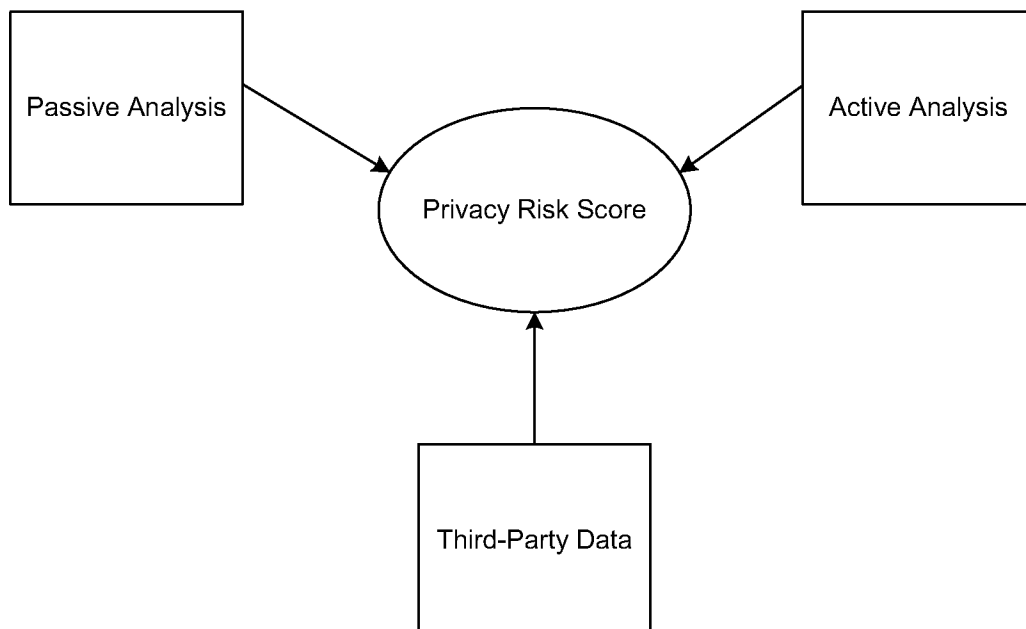


FIG. 14

10/11

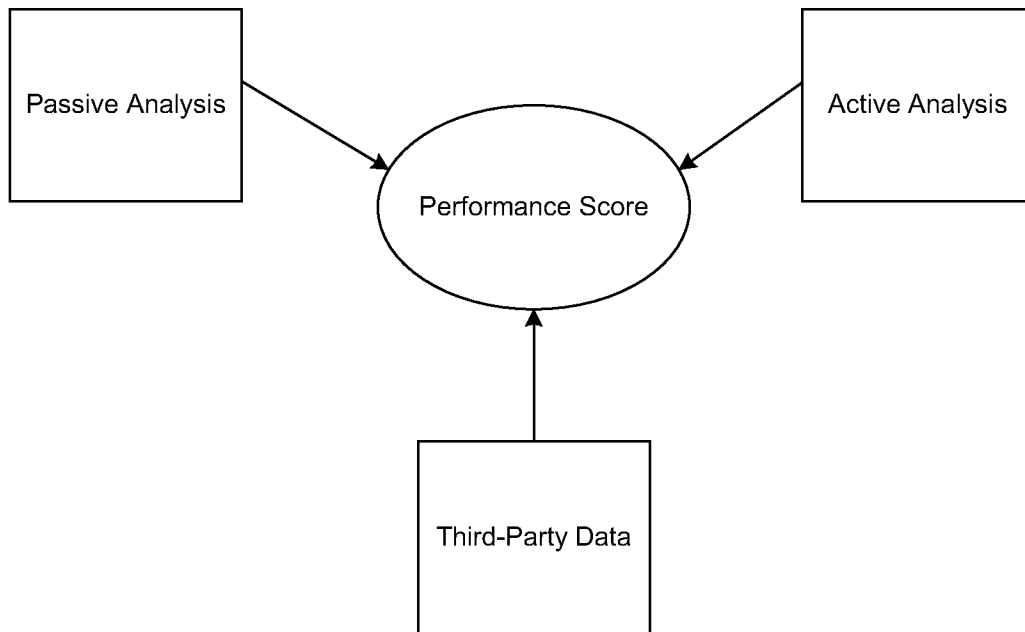


FIG. 15

11/11

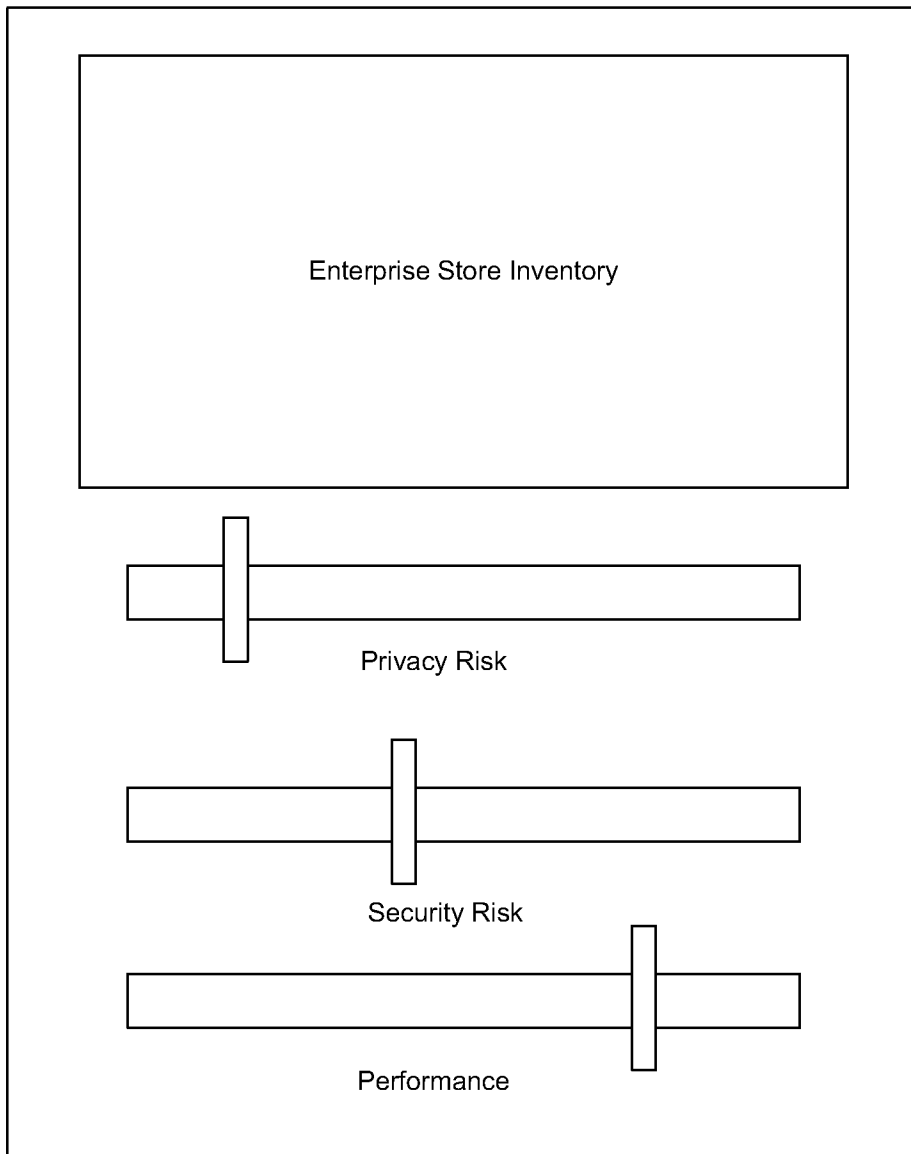


FIG. 16

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/062793

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/50 G06F21/57
ADD.

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)
G06F

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)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/145920 A1 (MAHAFFEY KEVIN PATRICK [US] ET AL) 16 June 2011 (2011-06-16) page 1, paragraphs 2,4,7 page 2, paragraph 24-26 page 3, paragraph 35 - page 4, paragraph 40 page 6, paragraph 49 - paragraph 57 page 10, paragraph 89 page 11, paragraph 99 - paragraph 104 page 12, paragraph 106 page 13, paragraph 109 page 16, paragraph 130 - page 17, paragraph 135 page 18, paragraph 141 - page 19, paragraph 144 page 22, paragraph 161 - paragraph 165 page 26, paragraph 186 page 30, paragraph 213 - page 31, paragraph 216 page 33, paragraph 225	1-84



Further documents are listed in the continuation of Box C.



See patent family annex.

* 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

25 February 2013

Date of mailing of the international search report

07/03/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Arbutina, Ljiljana

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2012/062793

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 36, paragraph 244 - paragraph 248 page 38, paragraph 259 - paragraph 262 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/062793

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011145920	A1	16-06-2011	NONE
