

smart devices. As mobile smart devices become even "smarter" and more complex, there will be a greater number of possible ways for something to go wrong with them. Currently, troubleshooting is a labor intensive proposition for carriers, it does not produce extra sales, and it takes away from employee time to generate sales.

[0016] Currently, there is not an easy and efficient way to scan a mobile smart device for malware and other viruses. The usual approach is to connect the mobile smart device to a laptop or desktop computer to perform such scans. Further, these scans must be carried out with the active participation of the computer user.

[0017] Typically, when a mobile smart device is being charged, it is usually dead time with respect to its user being able to use the device because it is tethered to a socket or computer by a charging cord. Further, mobile smart devices are almost totally unusable when they are being charged using a charging pad. This is why many people charge these devices at night or when they know they do not need to use them. It would be very advantageous to be able to use the charging time more efficiently and conduct malware and virus scans while the mobile smart device is being charged.

[0018] There is the need for a system and method that enables bidirectional trust between downloaded applications and the mobile smart devices onto which these applications are downloaded so that the mobile smart device can trust the downloaded applications are authentic and the downloaded applications can trust the mobile smart device is authorized to download them. There also is a need for an inexpensive mobile device that can be used for charging a mobile smart device and while charging scan and identify malware and other viruses that are on the mobile device.

Summary of the Invention

[0018a] According to a first aspect of the present invention, there is provided a computer-implemented system for electrically charging an electronic device and scanning the electronic device for at least malicious software ("malware") during at least a portion of the time period the computer-implemented system electrically charges the electronic device, comprising:
a power source connector for connecting the computer-implemented system to a power source;
an electrical power converter connected to the power source connector for converting the electrical power input to the power source connector to electrical power suitable for input to the electronic device for charging an electrical power storage means of the electronic device;

a controller for controlling operations of the computer-implemented system for at least scanning the electronic device for at least malware during at least a portion of the time period the computer-implemented system electrically charges the electronic device; a system memory connected to the controller for storing at least computer programs and data for at least scanning the electronic device for at least malware during at least a portion of the time period the computer-implemented system electrically charges the electronic device; a secure digital card connected to the controller for storing at least an operating system computer-based security programs, and on-device database for the computer-implemented system at least scanning the electronic device for at least malware during at least a portion of the time period the computer-implemented system electrically charges the electronic device; and an electronic device connector of the computer-implemented system for connecting the computer-implemented system to the electronic device for providing converted electrical power to the electronic device suitable for charging the electrical power storage means thereon and for bidirectional communications between the computer-implemented system and electronic device for at least scanning the electronic device for at least malware during at least a portion of the time period the computer-implemented system electrically charges the electronic device and providing scan results from the electronic device to the computer-implemented system for storage on the secure digital card.

[0018b] According to a second aspect of the present invention, there is provided a computer-implemented system for scanning the electronic device for at least malicious software ("malware") using at least a quick scan followed by a comprehensive full scan, comprising:
a controller for controlling operations of the computer-implemented system for at least the quick scan and comprehensive full scan of the electronic device for at least malware;
a system memory connected to the controller for storing at least computer programs and data for conducting the quick scan and comprehensive full scan of the electronic device for at least malware;
a secure digital card connected to the controller for storing at least an operating system, computer-based security programs, and on-device database for conducting the quick scan and comprehensive full scan of the electronic device for at least malware; and
a transceiver connected to the controller for wireless bidirectional communications between the computer-implemented system and the electronic device for conducting the quick scan and

comprehensive scan of the electronic device for at least malware and receiving scan results from the electronic device for storage on the secure digital card.

[0018c] According to a third aspect of the present invention, there is provided a computer-implemented method for electrically charging an electronic device and scanning the electronic device for at least malicious software ("malware") during at least a portion of the time period the computer-implemented system electrically charges the electronic device, comprising the steps of:

(a) connecting an electrical power source to an electrical power input connector of a charging/scanner device incorporated in first hardware device with the charging/scanner device for scanning the electronic device for malware while electrically charging electronic device, with the charging/scanner device including at least an electrical power converter, a controller, a system memory, a secure digital card, and an electronic device connector for connecting the scanning/charging device to the electronic device;

(b) converting with the electrical power converter the electrical power input to the scanning/charging device to electrical power suitable for input to the electronic device for charging an electrical power storage means of the electronic device;

(c) connecting the electronic device connector of the scanning/charging device to the electronic device for

(1) providing to the electronic device converted electrical power suitable for charging electrical power storage means of the electronic device, and

(2) establishing bidirectional communications over the connected electronic device connector for at least scanning the electronic device for at least malware during at least a portion of the time period the scanning/charging device electrically charges the electronic device and receiving scan results from the electronic device;

(d) scanning under the control of the controller the electronic device for at least malware during at least a portion of the time period the scanning/charging device electrically charges the electronic device according to,

(1) computer programs and data stored in a system memory, and

(2) an operating system, computer-based security programs, and on-device database on a secure digital card;

(e) receiving at the scanning/charging device malware scan results from the electronic device over the connected electronic device connector; and

(f) displaying the malware scan results using a status indicator associated with the first hardware device.

[0018d] According to a fourth aspect of the present invention, there is provided a computer-based system for determining a bidirectional trust between an electronic device and computer-based applications downloaded to such electronic device, comprising:

(a) a scanning device that includes being removably connected to the electronic device, with the scanning device for scanning the electronic device for malicious software ("malware") and receiving scan results that indicate whether the electronic device is compromised by having malware thereon or not compromised by being free of malware; and

(b) an internal network including at least,

(1) a server that includes at least a frontend server and a backend server, with the frontend server for receiving requests from and providing responses to customer input devices external to the internal network, and with the backend server for bidirectional communications with the scanning device for receiving at least scan results from the scanning device and transmitting at least computer software updates to the scanning device,

(2) an internal network database connected to the frontend server and backend server for storing at least customer information, electronic device information, and scan results,

(3) a certification authority for transmitting certificate information to the backend server and certificate information to the scanning device through the backend server for establishing secure communications between the scanning device and the backend server, and

(4) an authentication means for controlling authenticated communications between customer input devices external to the internal network and the frontend server.

[0018e] According to a fifth aspect of the present invention, there is provided a computer-based method for determining if a computer-base application downloaded by an electronic device can be a trusted application to be run on the electronic device, comprising the steps of:

(a) publishers of downloadable computer-based applications transmitting to an internal network publisher identification information for each of a specific publisher's downloadable computer-based applications, with the internal network storing the publisher identification information in an internal network database associated with information for each specific publisher downloadable computer-based application;

(b) connecting a scanning device to the electronic device for scanning for malware and the scanning device receiving scan results that indicate whether the electronic device is compromised by having malware thereon or not compromised by being free of malware, and the scanning device storing the scanning results thereon, with the scanning device determining at least one computer-based application downloaded to the electronic device and storing at least publisher identification information associated with the at least one downloaded computer-based application;

(c) the scanning device establishing a secure connection with the internal network that is remote from the scanning device and connecting to the internal network database storing the publisher identification information associated with each specific publisher downloadable computer-based application and querying the internal network database for the publisher identification information related to the at least one computer-based application downloaded to the electronic device identified in step (b);

(d) the internal network database responding to the query from the scanning device at step (c) and transmitting to the scanning device the publisher identification information related to the at least one computer-based application downloaded to the electronic device identified in step (b); and

(e) the scanning device comparing the publisher identification information received from the internal network database with publisher identification information associated with the at least one computer-based application downloaded to the electronic device identified in step (b) and if the publisher identification information matches determining the at least one computer-based application downloaded to the electronic device identified in step (b) is a valid/trusted computer-based application and usable by the electronic device and if the publisher identification information does not match determining the at least one computer-based application downloaded to the electronic device identified in step (b) is a invalid/not trusted computer-based application and not usable by the electronic device.

[0018f] According to a sixth aspect of the present invention, there is provided a computer-based method for determining if a computer-base application downloaded by an electronic device can trust the electronic device is authorized to receive the downloaded computer-based application, comprising the steps of:

(a) connecting a scanning device to the electronic device for scanning for malware and the scanning device receiving scan results that indicate whether the electronic device is compromised by having malware thereon or not compromised by being free of malware, and the scanning device storing the scanning results thereon, with the scanning device determining at least one computer-based application downloaded to the electronic device and the electronic device identification information;

(b) the scanning device establishing a secure connection with an internal network that is remote from the scanning device, and reporting the scan results and the electronic device identification information to the internal network;

(c) the internal network storing the scan results and electronic device identification information in a network database and associating therewith application publisher information for the at least one computer-based application downloaded to the electronic device;

(d) the internal network generating a service key related to the at least one computer-based application and storing the service key with the application publisher information in the network database and sending the service key to the application publisher remote from the internal network;

(e) the at least one computer-based application identified in step (a) establishing a connection from the electronic device to an application publisher using a wireless connection established through the electronic device and transmitting at least login information, a request to login to the application by the electronic device, the electronic device identification information, and a request for verification information to be sent to the internal network;

(f) the application publisher establishing a connection with the internal network and transmitting verification information to the internal network, with the verification information including at least the electronic device identification information and service key;

(g) the internal network receiving the verification information and comparing the verification information with the electronic device identification information and service key stored in the network database, and if the verification information matches then step (i) and if the verification information other than matches then step (h);

(h) the internal network transmits to the application publisher that a verification process ends because the electronic device identification information or service key other than matches electronic device identification based information or service key stored in the network database;

(i) the internal network transmitting to the application publisher a status of the electronic device based on scan results which includes at least the electronic device is compromised if the electronic device includes at least malware thereon or not compromised if the electronic device does not include at least malware thereon; and

(j) the publisher granting or denying the login request by the electronic device based on the status transmitted by the internal network to the publisher at step (i).

[0019] The Embodiments of the present invention ~~is~~are directed to a system and method that ~~will~~may enable users of mobile smart devices, such as cellular phones, PDAs, iPads, smartphones, mobile payment systems, e.g., point of sale systems (wired and wireless), mobile healthcare systems, handheld law enforcement systems, or other types of tablet devices, to trust download applications are authentic and for download applications to trust the mobile smart device onto which they are downloaded is authorized to download the applications. The system and method according to embodiments of the present invention are in part implemented through a secure charger that charges the mobile smart device and while charging it scans for malware and other viruses in the applications and the OS on the

mobile smart device. This helps to troubleshoot the mobile smart device so it ~~will~~may operate properly.

[0020] The system and method according to embodiments of the present invention ~~will~~can validate the authenticity of applications that have been downloaded to a mobile smart device to prevent counterfeit applications from being used on mobile devices and infecting them. According to embodiments of the present invention, when the secure charger scans for malware or other type of virus, it ~~will~~may access all the applications that have been downloaded to the mobile smart device. For mobile devices operating on an Android-based system, it ~~will~~would mean embodiments of the present invention ~~will~~may access the application package ("APK") files of every application. Since each of the applications is signed, the mobile smart device can make assumptions regarding the identity of the entity that published the application. ~~The Embodiments of the present invention uses~~use this information to verify that the signatures are not only valid but correspond to the appropriate application publisher, which permits verification of the authenticity of an application.

[0021] The system and method according to embodiments of the present invention ~~creates~~create a system database of applications, identifying information, and the appropriate application publishers. This information is stored at a remote location accessible through a remote system server. Preferably, application publishers will cooperate to facilitate the creation and population of this system database with publisher information. The system database also ~~will~~may be populated with popular applications in the marketplace, and the system administrator can verify the publisher information and add it to the database.

[0022] Typically, counterfeit applications do not have the appropriate publisher information associated with them. With the creation of the system database discussed above, when a downloaded application needs to be verified, the secure charger ~~will~~may send application information to the remote system server. The remote system server connects to the system database and the server ~~will~~may respond with the appropriate author's/publisher's public key for the secure charger to conduct the verification process. The secure charger ~~will~~may save the public keys which ~~will~~may enable the secure charger to carry out verifications itself in the future.

[0023] The system and method according to embodiments of the present invention permit applications to trust the mobile smart devices onto which they are downloaded is authorized to

receive the downloaded application. Typically, when a mobile smart device uses an application accessible through a remote service, the application author/publisher and the service providing the application have to assume the mobile smart device is secure, i.e., it is a device authorized to receive the application download; however, there is currently no way to do this.

[0024] According to system and method in embodiments of present invention, application authors/publishers and services that provide the applications for download can connect to the remote location to verify the mobile smart device is secure. This is accomplished by the secure charger reporting scan results to the remote server at the remote location every time it conducts a scan. The scan results ~~will~~may indicate the status of the mobile smart device as either compromised or not. The remote system server ~~will~~may store this information for logging and reporting, and to inform application authors/publishers and services whether the mobile smart device is secure.

[0025] ~~The~~Embodiments of the present invention ~~provides~~provide a powerful capability for service writers because it gives them security guarantees and limits the ability of attackers to impersonate a mobile smart device. Although an attacker may attempt to impersonate a mobile smart device to test the defenses of the remote system server, the implementation of the present invention ~~will~~may enable the service to check to determine if the attacker is an authorized mobile smart device. If it is not, the mobile smart device ~~will~~may be viewed as "compromised" and not a trusted mobile smart device. Once a mobile smart device is determined to be "compromised" (or "not recently scanned"), the application author/publisher and/or service either will deny access to the application or take other punitive actions, such as issuing warnings, charging fees, or other types of actions to give notice that access is denied.

[0026] For purposes of the present invention, a "service" preferably is a "web service." The web service is an application that exists in a distributed environment, such as the Internet. The web service ~~will~~may effect communication between two electronic devices over the Internet. The web service will accept a request, perform the function based on the request, and return a response. The request and response may use a protocol, such as HTTP.

[0027] For purposes of the present invention, a "service writer" is a company or individual that provides the web service.

[0028] The secure charger according to embodiments of present invention includes a mobile smart device charging cable and embedded electronics that will perform forensic and behavior analysis of the mobile smart device while it is charging. As such, system and method according to embodiments of the present invention ~~will~~may be able to observe malicious behavior, malicious software, modifications to the mobile smart device OS, and unwanted device

communications. The secure charger ~~will~~may identify unusual patterns of device communications activities representing attempts to steal or redirect personal data on the device.

[0029] The system according to embodiments of the present invention resides outside of the mobile smart device system so it is able to interface with mobile smart devices at a very low level. As such, malware ~~will~~may not be able to "lie" to system of the present invention.

[0030] The scanning function that was described with respect to the secure charger may also be implemented by a separate wireless scanning device. The wireless device ~~will~~may include a hardware component and a software component. The wireless hardware component may use a radio frequency ("RF") connection including, but not limited to, an 802.1 lx or Bluetooth connection. The hardware component may be in the form of an 802.1 lx wireless access point ("WAP") or a Bluetooth dongle.

[0031] The software component located on the mobile smart device acts as a proxy for an authenticated hardware device to perform analysis and run scans. Authentication is achieved by having the hardware component present a signed certificate and the software component will validate the signature.

[0032] The system and method according to embodiments of the present invention provide a means by which a mobile smart device can trust a downloaded application.

[0033] The system and method according to embodiments of the present invention provides a means by which a downloaded application can trust that the mobile smart device on which it is downloaded is authorized to download the application.

[0034] The system and method according to embodiments of the present invention ~~provides~~provide means by which a single device can charge a mobile smart device and also scan the mobile device for malware or other viruses while mobile smart device is charging.

[0035] The system and method according to embodiments of the present invention also provide means by which a separate scanning device can be used to wirelessly scan a mobile smart device for malware and other viruses.

[0036] The system and method of the present invention will be described in greater detail in the remainder of the specification referring to the drawings.

Brief Description of Drawings

[0037] Figure 1 shows a representative drawing of the system of the present invention for implementing bidirectional trust between a mobile smart device and downloaded applications.

[0038] Figure 2 shows a representative drawing of the secure sockets layer ("SSL") connection shown in Figure 1.