

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-conducting an integrity analysis scan of 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~~ conducting the integrity analysis scan of the electronic device with an electronic device baseline ~~for at least malware~~ during at least a portion of the time period the computer-implemented system electrically charges the electronic device and for sending scan results to a backend server and receiving updates from the backend server; a system memory connected to the controller for storing at least computer programs and data for at least ~~scanning~~ conducting the integrity analysis scan of the electronic device with the electronic device baseline ~~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~~ conducting the integrity analysis scan of the electronic device with the electronic device baseline ~~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~~ conducting the integrity analysis scan of the electronic device with the electronic device baseline ~~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.~~

[0018] ~~be~~ According to a ~~third~~ second aspect of the present invention, there is provided a computer-implemented method for electrically charging an electronic device and ~~scanning~~ conducting an integrity analysis of 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 ~~a first hardware device with the charging/scanner device for scanning~~ conducting the integrity analysis of the electronic device with an electronic device baseline ~~for malware~~ while electrically charging ~~the~~ the 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~~ conducting the integrity analysis of the electronic device with an electronic device baseline ~~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~~ conducting the integrity analysis of the electronic device with an electronic device baseline and sending scan results to a backend server and receiving updates from the backend server ~~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-integrity analysis~~ results from the electronic device over the connected electronic device connector; and (f) displaying the ~~malware scan-integrity analysis~~ results using a status indicator associated with the ~~scanning/charging~~ 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.

[0018] 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] Embodiments of the present invention are directed to a system and method that 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

CLAIMS:

1. A computer-implemented system for electrically charging an electronic device and ~~scanning-conducting an integrity analysis scan of 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-conducting the integrity analysis scan of the electronic device with an electronic device baseline for at least malware~~ during at least a portion of the time period the computer-implemented system electrically charges the electronic device and for sending scan results to a backend server and receiving updates from the backend server;

a system memory connected to the controller for storing at least computer programs and data for at least ~~scanning-conducting the integrity analysis scan of the electronic device with the electronic device baseline 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-conducting the integrity analysis scan of the electronic device with the electronic device baseline 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-conducting the integrity analysis scan of the electronic device with the electronic device baseline 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.

2. The computer-implemented system as recited in claim 1, wherein the power source includes an external power source.
3. The computer-implemented system as recited in claim 1, wherein the power source converter includes a transformer for converting alternating current (“AC”) to direct current (“DC”).
4. The computer-implemented system as recited in claim 1, wherein the controller includes a computer processing unit (“CPU”).
5. The computer-implemented system as recited in claim 1, wherein the system memory includes a random access memory (“RAM”).
6. The computer-implemented system as recited in claim 5, wherein the RAM includes storing running program code, data, and volatile system files.
7. The computer-implemented system as recited in claim 1, wherein the computer-based security programs include security analysis computer-based programs.
8. The computer-implemented system as recited in claim 1, wherein the computer-implemented system includes scanning for at least one from a group that includes viruses, malicious software (“malware”) rootkits, counterfeit software, system configuration and setting changes, and exploits.
9. The computer-implemented system as recited in claim 1, wherein the computer-implemented system includes a status indicator to indicate whether returned scan results have identified ~~malware on~~ at least one comparison difference in conducting the baseline scan of the electronic device thereby indicating the electronic device is compromised.
10. The computer-implemented system as recited in claim 9, wherein the status indicator includes at least one light emitting diode (“LED”) light.
11. The computer-implemented system as recited in claim 10, wherein the status indicator includes a liquid crystal display (“LCD”) that will indicate thereon at least whether returned scan results have identified ~~malware on~~ at least one comparison difference in conducting the baseline scan of the electronic device thereby indicating the electronic device is compromised.
12. The computer-implemented system as recited in claim 1, wherein the electronic device includes a mobile smart device.
13. The computer-implemented system as recited in claim 12, wherein the mobile smart device is selected from a group including at least cellular phones, personal digital assistants, tablet devices, smartphones, mobile payment systems, mobile healthcare systems, handheld law, and enforcement systems.

14. — 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.

15. — The computer-implemented system as recited in claim 14, wherein the controller includes a computer processing unit ("CPU").

16. — The computer-implemented system as recited in claim 15, wherein the system memory includes a random access memory ("RAM").

17. — The computer-implemented system as recited in claim 16, wherein the RAM includes storing running program code, data, and volatile system files.

18. — The computer-implemented system as recited in claim 17, wherein the computer-based security programs include security analysis computer-based programs.

19. — The computer-implemented system as recited in claim 14, wherein the computer-implemented system includes scanning for viruses.

20. — The computer-implemented system as recited in claim 14, wherein the computer-implemented system includes a status indicator to indicate whether returned scan results have identified malware on the electronic device.

21. — The computer-implemented system as recited in claim 20, wherein the status indicator includes at least one light emitting diode ("LED") light.

22. — The computer-implemented system as recited in claim 20, wherein the status indicator includes a liquid crystal display ("LCD") that will indicate thereon at least whether returned scan results have identified malware on the electronic device.

23. ~~The computer-implemented system as recited in claim 14, wherein the electronic device includes a mobile smart device.~~

24. ~~The computer-implemented system as recited in claim 23, wherein the mobile smart device is selected from a group of including at least cellular phones, personal digital assistants, tablet devices, smartphones, mobile payment systems, mobile healthcare systems, and handheld law and enforcement systems.~~

1425. A computer-implemented method for electrically charging an electronic device and scanning-conducting an integrity analysis of 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 a first hardware device with the charging/scanner device for scanning-conducting the integrity analysis of the electronic device with an electronic device baseline ~~for malware~~ while electrically charging the 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-conducting the integrity analysis of the electronic device with an electronic device baseline ~~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-conducting the integrity analysis of the electronic device with an electronic device baseline and sending scan results to a backend server and receiving updates from the backend server 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~~integrity analysis results from the electronic device over the connected electronic device connector; and

(f) displaying the ~~malware scan~~integrity analysis results using a status indicator associated with the scanning/charging device.

~~1526.~~ The computer-implemented method as recited in claim ~~25~~14, wherein the status indicator includes at least one light emitting diode (“LED”).

~~1627.~~ The computer-implemented method as recited in claim ~~25~~14, wherein the status indicator includes a liquid crystal display (“LCD”) that will indicate thereon at least whether the returned scan results have identified ~~malware on~~at least one comparison difference in conducting the baseline scan of the electronic device thereby indicating the electronic device is compromised.

~~1728.~~ The computer-implemented method as recited in claim ~~25~~14, wherein the method includes scanning the electronic device for viruses during at least a portion of the time period the scanning/charging device electrically charges the electronic device.

29. — 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.~~

~~30. — The computer-based system as recited in claim 29, wherein the electronic device connects to the backend server through a wireless connection.~~

~~31. — The computer-based system as recited in claim 30, wherein the wireless connection between the electronic device and the backend server includes a wireless Internet connection.~~

~~32. — The computer-based system as recited in claim 31, wherein the scanning device connects to the backend server through the wireless Internet connection of the electronic device.~~

~~33. — The computer-based system as recited in claim 29, wherein the certification authority provides at least predetermined certificate authority certificates to the backend server, and provides at least a predetermined certificate authority certificate and private keys to the scanning device for the backend server to compare the certificate authority certificate it received from the certification authority with the certificate authority certificate it received from the scanning device.~~

~~34. — The computer-based system as recited in claim 29, wherein the internal network database includes at least a customer information database, an electronic device information database, and a scan database.~~

~~35. — The computer-based system as recited in claim 34, wherein the customer information database is for storing customer information that includes at least information associating a customer with one or more electronic devices and customer settings for interacting with the internal network.~~

~~36. — The computer-based system as recited in claim 34, wherein the electronic information database is for storing electronic device information that includes at least information for all electronic devices supported by the internal network.~~

~~37. — The computer-based system as recited in claim 36, wherein for each electronic device supported by the internal network, the electronic information database includes at least the computer software version of the computer software on the electronic device, an updated baseline of a computer software platform on the electronic device, and recover images for the electronic device.~~

38. — The computer-based system as recited in claim 29, wherein the scan database is for storing scan results received from the scanning device which include whether an electronic device is compromised or not compromised.

39. — The computer-based system as recited in claim 38, wherein the scan database includes storing for each electronic device at least a list of computer-based applications on the electronic device, a list of files and hashes on the electronic device, a time and date of each scan, and a type of each scan.

40. — The computer-based system as recited in claim 29, wherein the scan device includes scanning for viruses.

41. — 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.

42. —The computer-based method as recited in claim 41, wherein connecting the scanning device to the electronic device includes wirelessly connecting the scanning device to the electronic device using an 802.11 radio frequency ("RF") connection or Bluetooth connection.

43. —The computer-based method as recited in claim 42, wherein the electronic device connects to the internal network through a wireless connection.

44. —The computer-based method as recited in claim 43, wherein the wireless connection between the electronic device and internal network includes a wireless Internet connection.

45. —The computer-based method as recited in claim 44, wherein the scanning device connects to the internal network through the wireless Internet connection of the electronic device.

46. —The computer-based method as recited in claim 41, wherein publisher identification information stored in the internal network database includes publisher signature information.

47. —The computer-based method as recited in claim 41, wherein the publisher signature information includes publisher public keys.

48. —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).

49. — ~~The computer-based method as recited in claim 48, wherein step (h) includes permitting the application publisher to resubmit the electronic device identification information and service key a predetermined number of times before the verification process ends.~~

50. — ~~The computer-based method as recited in claim 49, wherein step (h) includes permitting the application publisher to resubmit the electronic device identification information and service key three times or less before the verification process ends.~~

51. — ~~The computer-based method as recited in claim 48, wherein the status of the electronic device based on scan results includes "not recently scanned" if the electronic device has not been scanned within at least one (1) day.~~

52. — ~~The computer-based method as recited in claim 51, wherein if the status of the electronic device is "not recently scanned," the status of the electronic device is determined as compromised.~~

53. — ~~The computer-based method as recited in claim 48, wherein the application publisher grants the login request at step (j) if the scan results received from the internal network include electronic device is not compromised.~~

54. — ~~The computer-based method as recited in claim 48, wherein the application publisher denies the login request at step (j) if the scan results received from the internal network include electronic device is compromised.~~