CLAIMS

What it claimed is:

1. A method for enhancing the security of a mobile device running a mobile application and communicating with a server, the method comprising:

on the mobile device, continuously monitoring a plurality of parameters of the mobile device associated with installing, loading or running the mobile application for one or more predetermined triggering events;

on the mobile device, upon detecting one more of said triggering events, executing a fingerprinting routine configured to obtain a current state of a plurality of device fingerprint attributes of the mobile device;

transmitting said current state of the plurality of device fingerprint attributes of the mobile device to a risk engine running on the server;

analyzing with said risk engine said current state of the plurality of device fingerprint attributes of the device to obtain device intelligence information, said analyzing including comparing said current state of the plurality of device fingerprint attributes of the mobile device with a previously obtained state of the plurality of device fingerprint attributes of the mobile device associated with installing, loading or running the mobile application on the mobile device; and

transmitting said device intelligence information to said mobile device; and

on the mobile device, undertaking one or more actions based on the intelligence information received from the server.

2. The method according to claim 1 further comprising saving to database information indicative of the current state of a plurality of device fingerprint attributes of the mobile device.

3. The method according to claim 2 wherein said information indicative of the current state of a plurality of device fingerprint attributes of the mobile device is a delta between the mobile device fingerprint attributes at the current state and at a previous state of the mobile device.

4. The method according to claim 1 wherein said device intelligence information includes a quantitative risk score that indicates the level of risk associated with the current mobile application session on the mobile device.

5. The method according to claim 1 wherein said device intelligence information includes qualitative information indicative of what types of trigger events are associated with the current mobile application session on the mobile device.

6. The method according to claim 1 wherein said one or more actions include one or more of the following: continue monitoring the mobile device, send the user a warning, terminate a user running the mobile application, and shut down the mobile application.

7. The method according to claim 1 wherein said one or more predetermined triggering events include one or more event types selected from a list consisting of the following events at the mobile device: a risk module is installed; a risk module is initialized; the mobile application is resumed; a display configuration has been changed; a screenshot is taken; a GPS provider change is detected; a network change is detected; and a change in tools is detected.

8. The method according to claim 1 wherein said plurality of device fingerprint attributes of the mobile device includes fingerprint attributes from one or more attribute categories selected from a list consisting of: device hardware; network; software; screen; and location.

9. A system for enhancing security of a mobile device running a mobile application and communicating with a server running a risk engine platform, the system comprising:

a mobile application running on the mobile device, the mobile application configured to continuously monitor a plurality of parameters at the

mobile device associated with the mobile application for one or more predetermined triggering events, and upon detecting one or more of said triggering events, execute a fingerprinting routine at the mobile device configured to obtain a current state of a plurality of device fingerprint attributes of the mobile device, and transmit said current state of the plurality of device fingerprint attributes of the mobile device to a risk engine running on the server; and

running said risk engine platform to analyze the received current state of the plurality of device fingerprint attributes of the mobile device to obtain device intelligence information, said analysis including comparing said current state of the plurality of device fingerprint attributes of the mobile device with a previously obtained state of the plurality of device fingerprint attributes of the mobile device associated with installing, loading or running said mobile application at the mobile device, and transmit said device intelligence information to said mobile device, wherein said mobile application is further configured to undertake one or more actions at the mobile device based on the intelligence information received from the server platform.

10. The system according to claim 9 wherein said server is further configured to save to a database information indicative of the current state of a plurality of device fingerprint attributes of the mobile device.

11. The system according to claim 10 wherein said information indicative of the current state of a plurality of device fingerprint attributes of the mobile device is a delta between the device fingerprint attributes at the current state of the mobile device and at a previous state of the mobile device.

12. The system according to claim 9 wherein said device intelligence information includes a quantitative risk score that indicates the level of risk associated with the current mobile application session at the mobile device.

13. The system according to claim 9 wherein said device intelligence information includes qualitative information indicative of what types of trigger events are associated with the current mobile application session at the mobile device.

14. The system according to claim 9 wherein said one or more actions include one or more of the following events at the mobile device: continue to monitor the mobile device, send the user a warning, terminate a user running the mobile application, and shut down the mobile application.

15. The system according to claim 9 wherein said one or more predetermined triggering events include one or more event types selected from a list consisting of the following events at the mobile device: a risk module is installed; a risk module is initialized; the mobile application is resumed; a display configuration has been changed; a screenshot is taken; a GPS provider change is detected; a network change is detected; and a change in tools is detected.

16. The system according to claim 9 wherein said plurality of device fingerprint attributes includes one or more fingerprint attributes types from a list consisting of the following attributes of the mobile device: device hardware - device brand, device name, device model, IMEI, battery level, battery temperature, brand, manufacturer, model, hardware, host, device, ID and CPU; network - carrier name, carrier country, battery technology, battery voltage, battery health, carrier country code, carrier network code, Wi-Fi name, Wi-Fi IP address and WIFI mac address; software - OS version, merchant app version, version incremental, version release and version codename; screen - screen resolution, screen size, pixel density and display; location - GPS country, GPS coordinates, IP country and IP address; and miscellaneous - timezone, user language and user agent.