

METHOD TO IDENTIFY UNIQUENESS OF SMART DEVICES AND THEIR COMPONENTS

FIELD OF THE INVENTION

The invention belongs to the field of emerging technology for identifying the uniqueness of smart devices and their components.

BACKGROUND OF THE INVENTION

With the popularization of smart phones and smart devices, the sales of insurance products for the devices are also increasing. The object of this type of service is often a piece of hardware in a smart device, such as a screen, battery, or memory. Therefore, the insurance companies need to confirm whether the customer has replaced the original components of the devices before issuing an insurance company.

The usual practice is to require users to provide serial numbers, such as mobile phone IMEI numbers. The problem with this method is that the user cannot provide the serial numbers of the components and accessories in the smart device, which makes it possible for the users to benefit from replacing the accessories and making claims.

SUMMARY OF THE INVENTION

The present invention discloses an analysis and processing method for identifying uniqueness of smart devices and their components. The analysis and processing method at least includes the following steps:

S100: the client App collects the device uptime from the system API;

S200: the client App collects the device location information from the GPS unit;

S300: the client App collects the connection information of the device based on the device's Bluetooth and WiFi data;

S400: the client App collects the device's battery power level at the first and the second timestamp, then calculate the battery capacity of the device;

S500: the client App collects the device make, model, and serial numbers through system API;

S600: the client App sends the data collected in step S100 to step S500 to the server;

S700: based on the received data, the server verifies identity of the device and its components, and access the probability that the original components were replaced;

S800: the server sends the recommended results to the client App, and guides the customer to provide additional information.

S900: when providing hardware repair and replacement services, verify whether the components have been replaced.

According to a preferred embodiment, the evaluation process of the possibility of components replacement of the device in step S700 includes: evaluating whether the user has shut down or restarted the hardware system of the device recently through the uptime of the system captured in step S100; based on the device location information and user address information obtained in step S200; assess the environment of the user based on the Bluetooth and WiFi connection information obtained and flag high-risk locations in step S300 and step S400; in step S500, complete the evaluation of whether the hardware model and serial number are original hardware.

According to a preferred embodiment, the analysis and processing method further includes the step of S800 where the server sends the evaluation result of step S700 to the client App, and guides the user to perform the follow up operation.

According to a preferred embodiment, the analysis and processing method further includes the step of S900: When a repair and replacement service is provided for the hardware, verify whether the hardware has been replaced.

According to a preferred embodiment, in the step S100, the client reads the uptime of the device system through the device software API.

According to a preferred embodiment, in the step S200, the positioning unit is not limited to a GPS positioning module.

The benefits of the present invention are:

- 1) It can automatically, conveniently and reliably evaluate the risk of users replacing smart device hardware and components;
- 2) Greatly reduce the risk of customers directly requesting repairs after concealing the replacement of its hardware and components;
- 3) Through GPS positioning, Bluetooth and WiFi address analysis, locate service providers that assists insurance fraudulent claims;
- 4) By reading the hardware information, judge whether the device is within the scope of maintenance or insurance coverage.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the analysis and processing method of the system;

FIG. 2 illustrates the processing flow of an implementation example.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will be further described hereinafter with reference to the accompanying drawings. It is to be understood that specific embodiments described herein are only intended to explain the present invention, and are not taken to limit the present invention. Further, it will be appreciated that the examples provided represent only one of many possible implementations of the present invention.

Referring to FIG. 1, the present invention discloses a process for identifying uniqueness of the devices and whether the hardware of a smart device is exchanged, and the method at least includes the following steps:

Step S100: Configure the client App on the smart device to collect the system uptime from the device. Preferably, in the step S100, the client App reads the system uptime and elapsed time from the device system through a system API.

Specifically, the system uptime and elapsed time in step S100 can be used to determine the time when the smart device was turned on or restarted last time. Smart devices cannot keep the device system running and detach the core components to the device. If the user has removed or replaced the core hardware, it must be done before the last system restart. Conversely, customers cannot replace any core hardware after the last system restart. The longer the system is up and alive, the lower the risk that the user replaced smart device hardware recently. Users who have restarted on the same day have a very high risk of replacing smart device hardware.

Insurance products designed for smart devices in the market, especially phone screen insurance, face a significant risk of customer fraud. Even if the insurance company determines the uniqueness of the user's mobile phone IMEI or Serial number used to activate the insurance policy through a system API, the user can also fraud the insurance claims by replacing the damaged accessories.

The specific steps to fraud insurance claims are: 1. The user finds a mobile phone with a broken screen; 2. The user replaces the broken screen of the mobile phone with an unbroken screen, and purchases a phone screen insurance for this phone; 3. The user changes the screen back to the broken screen, and submits a claim against the insurance company; 4. The

insurance company verifies that it is the covered phone, approves the claim, and the user gets a new screen or cash compensation.

In step 2 of the fraudulent claim process, the user needs to turn off the phone before detaching and replacing the phone screen. Normal users should not shut down or restart their phones regularly. Therefore, when an insurance company finds that the user has recently restarted the phone, it can be assumed that the user is more likely to fraud the phone insurance through the above method thus not providing coverage to the phone.

Smart devices (such as mobile phones, tablet computers) are usually waterproof under the condition of being undamaged and not repaired. After the equipment is repaired, it will lose its waterproof function. Thus when the equipment is intact, the user has no incentive to give up the waterproof function, and to profit from making a fraud insurance claim.

Step S200: The client App acquires device location from the positioning unit on the smart device. Preferably, in the step S200, the location can be derived from Bluetooth and WiFi signals and is not limited to the GPS module.

The GPS data in step 200 can be used to determine the current location of the user. By cross validation with other user information, such as home and office address, the algorithm determines the fraud risk of the user at the current location. Replacing smart device hardware components often requires professional tools, and ordinary users cannot complete it independently. For users whose current location is the user's home address, there is a lower risk of user fraud. For users currently at commercial addresses, especially near phone repair shops or at hotspot addresses there is a higher risk of user fraud.

Step S300: The client App obtains the connection information of the device based on the Bluetooth and WiFi data of the smart devices.

The short-range transmission of Bluetooth and WiFi collected in step 300 can be used to determine the current environment of the user. When users are in the same location, they can see the coverage of the same router WiFi signals, and mobile device Bluetooth signals. When a large number of devices are in the coverage for the same signal, it can be considered that the users are at the same location. When a large number of users try to purchase the insurance from the same location, there is a greater risk of fraud, such as a service provider that provides repairs and exchanges of hardware components.

Step S400: The client App calculates the current battery capacity of the device by checking the battery capacity at the first timestamp and at the second timestamp.

The battery capacity information in step 400 can be used to determine the user's battery life. The capacity and life of phone original batteries decrease with the number of charging

cycles. The battery capacity information can be used to determine whether the user has replaced the original battery.

Step S500: The client App obtains the device hardware model and serial number data through the device system API.

In step 500, the device model and serial number are extracted at the software level, and to determine whether it is original and whether it has been exchanged. When the service provider repairs and replaces the device and the components, the client App can compare the device model and serial number of the device recorded on the server side.

Step S600: The client App sends the data information collected in steps S100 to S500 to the server.

In step 600, the client App can send the information collected in the above steps to the server. In addition to the above information, the client App can also send the unique identification code of the device, the serial number of the device hardware, and the timestamp of the collected data to the server.

Further, the client App can perform asymmetric encryption on the information. Where only the server can decrypt the information securely and obtain the device information.

In some implementations, the client can encrypt the collected information in an audio, image or video format with a digital signature, which is captured by the second unit and transmitted to the server, for example, the encrypt the information in a two-dimensional QR code displayed on the screen of the target device, and then the photo is transmitted to the server through a second device.

Step S700: The server completes the evaluation of the risk that the hardware of the device is exchanged or replaced based on the received data from the previous steps .

Preferably, the evaluation process of the possibility that the hardware of the smart device is exchanged in the step S700 includes:

Based on the system uptime captured in step S100, the server checks whether the user has shut down or restarted the system of the device recently. The behaviour of removing or replacing the core hardware or component can only be performed when the system is shut down. Therefore, the longer system uptime, the lower the risk of users replacing the device hardware or component. Users who shut down or restarted the system on the same day are at a higher risk.

Based on the device location information and user address information obtained in step S200, an assessment of whether the device is in a high-risk location is completed.

Exchanging smart device hardware often requires professional tools, and ordinary users

cannot complete it independently. For users at their home address, there is a lower risk of insurance fraud. Users at a commercial address have a higher risk of changing the hardware of their smart devices.

Based on the Bluetooth and WiFi connection information obtained in step S300 , the relative position of the user is judged, and the evaluation of whether the device is in a high-risk location of hardware replacement is completed. This also reduces the risk that users visit certain high-risk locations where the service provider makes a profit by replacing the equipment hardware and making fraudulent insurance claims.

Based on the power information in step S400, it is evaluated whether the battery capacity information matches the device model and lifetime. And use this to determine whether the user has replaced the original battery, and whether the power consumption of the device hardware is normal.

Based on the hardware model and serial number information collected in step S500, the evaluation of whether the hardware model and serial number are original hardware is completed.

Step S800 : The server sends the evaluation result of step S700 to the client, and guides the user to the next step. When the risk is determined to be low, the client App recommends insurance and services to customers. When it is determined that the risk is high, insurance and services are not recommended to the user.

Step S900: When providing maintenance and replacement services for the hardware, the server verifies whether the hardware has been replaced. When providing services to the hardware at a later claim stage, the server compares the data collected through steps 100-500 before and verifies the risk determined in step 700 and also verifies whether the hardware is covered by the service.

In summary, the method of the present invention can automatically, conveniently, and reliably extract device information, and use this to determine the uniqueness of the device and the risk of the user replacing the smart device hardware.

The purpose of the present invention is to determine the risk of the user replacing the smart device hardware, rather than completely determining whether the user has replaced the smart device hardware. In a specific implementation case, a significant reduction in fraud effectively controls the risk of user fraud, thereby achieving the goal of overall product profitability.

The main risk is that professional service providers fraud insurance claims through professional means on a large scale. The present invention can effectively find and reduce such risks through GPS positioning, Bluetooth and WiFi address analysis.

IMPLEMENTATION EXAMPLE:

With reference to Figure 2, the present invention discloses an analysis and processing method for whether the hardware of a smart device is exchanged. This example will illustrate the application of the method for analysing whether the components of the device of the present invention are exchanged when applying for a phone screen insurance for an Android mobile phone and the system is Android10.

Step 1: The client reads the device's unique number AndroidID through the mobile phone system API. The specific reading method is :

```
val androidId = Settings.Secure.getString(contentResolver,Settings.Secure.ANDROID_ID)
```

The acquisition of the ID does not require additional permissions, and the unique identification of the identifier is guaranteed when the user does not reset the system.

Step 2: The client App reads the uptime information of the device system through the system API. The Android mobile phone system provides a variety of ways of system uptime, including `SystemClock.elapsedRealtime()` and `SystemClock.elapsedRealtime()`, both of which indicate the time after system boot. `uptimeMillis()` stops during deep sleep, `elapsedRealtime()` is not affected by system sleep.

`elapsedRealtime()` is more suitable for judging the real uptime of system operation after system boot. The method can obtain the system running time without special permission, and it is also unmodifiable and reliable.

Using the above methods, the client App can determine the user's last shut-down time and the usage time of the mobile phone. For users who have recently shut down and have not experienced a deep sleep cycle, the fraud risk is high, and the client does not show the user the option to purchase phone screen insurance.

Step 3: The client obtains the location information of the device through the device GPS, Bluetooth, WiFi and other data. When the user refuses to provide the corresponding information, risk can be high, and the client App does not show the user the option to purchase phone screen insurance.

After the user agrees to share the location information, the server side analyses the fraud risk of the user's location. Under normal circumstances, different users will not purchase phone screen insurance in the same location and within the coverage of the same Bluetooth or WiFi

signal source. When multiple users purchase phone screen insurance at the same location, it is likely that there is a repair service provider professionally providing mobile phone screen replacement at that location to fraud insurance. For these users, the server can build the corresponding phone ID, GPS location, WiFi address, and Bluetooth address blacklist. The client App does not show the users on the blacklist the option to purchase phone screen insurance.

Step 4: The client App calculates the current battery capacity of the device. When the user opens the client App, the first timestamp and the current battery level of the phone are recorded. When the user purchases the phone screen insurance, the second time stamp and the current mobile phone battery power are recorded.

By analysing the battery power difference of the phone between the two timestamps, the current battery capacity of the mobile phone can be estimated. The phone battery capacity decreases with the phone usage. Thus the client App can determine whether the user is using the phone normally by combining the phone model, user registration information, and analysing the current battery capacity.

Step 5: The client obtains the device hardware model and serial number through the system API. When a mobile phone of a specific manufacturer provides this information, the client can determine whether the device hardware is original, and record the hardware model and serial number, and determine whether the user has replaced the screen and other hardware when the mobile phone is repaired.

Step 6: The client App sends the collected information to the server. Based on the information, the server determines the risk that the user has exchanged the hardware of the device. The client cannot independently determine the fraud risk of location information such as GPS, Bluetooth, WiFi, so such information needs to be sent to the server for further analysis. The server also further verifies the information sent by the client App, and sends a confirmation message to the client App that the broken screen of the mobile phone covers the mobile phone.

Step 7: The server sends the risk assessment result to the client App, and guides the customer to perform operations. Depending on the product process of the client product, the user may need to check the screen of the phone, provide insurance policy information, or make a payment.

Step 8: When the insurance company provides repairs to the mobile phone, it verifies whether the hardware has been replaced. When repairing the mobile phone, the repairer can judge whether the user has changed the hardware of the device through the screws, internal originals, and whether there is water damage. For customers who have replaced the equipment

hardware by themselves, the insurance company can reject the user's claim application in accordance with the corresponding policy clauses.

The aforementioned basic examples of the present invention and each of its further alternative examples can be freely combined to form multiple embodiments, which are all applicable and claimed embodiments of the present invention. In the scheme of the present invention, each alternative example can be combined with any other basic examples and alternative examples arbitrarily. Those skilled in the art will know that there are numerous combinations.

The above descriptions are only the preferred embodiments of the present invention and are not intended to limit the present invention. Any modification, equivalent replacement and improvement made within the spirit and principle of the present invention shall be included in the protection of the present invention.

CLAIMS

1. A method for evaluating a risk of fraudulent claim for a hardware component in a smart device, wherein the method comprises the following steps:

Collecting the smart device's uptime from the smart device's API for determining when the smart device was turned on or restarted;

Acquiring the smart device's location information from a GPS unit for determining the degree of fraud risk of the current location;

Obtaining the location of the smart device from Bluetooth and/or WiFi data for determining the degree of fraud risk of the current location;

Calculating a current battery capacity of the smart device through a power of the smart device at a first timestamp and a power of the smart device at a second time stamp for determining whether a battery is original;

Obtaining the smart device's model and unique identifier data through the smart device's API;

Sending the data information collected in the above steps to a server; and

Evaluating the possibility that the hardware component of the smart device is exchanged based on the received data information, by the server.

2. The method according to claim 1, wherein the step of evaluating the possibility that the hardware component in the smart device is exchanged based on the received data information, by the server, comprises:

Evaluating whether the smart device has been shut down or restarted recently through the smart device's uptime captured from the smart device's API;

Based on the smart device's location information and the smart device user's registration information, completing the assessment of whether the smart device is in a high-risk location for hardware component replacement;

Based on the information obtained from GPS, Bluetooth, and/or WiFi connection information, determining the location of the smart device, and completing the assessment of whether the smart device is in a high-risk location for hardware component replacement;

Based on the battery capacity information, evaluating whether the battery capacity information is consistent with the smart device model and useful life; and

Based on the smart device's model and unique identifier data, evaluating whether the smart device is original.

3. The method according to claim 1 or 2, wherein the method further comprises the steps of:

Sending an evaluation result of the possibility that the hardware component of the smart device is exchanged to the smart device user by the server; and

Guiding the smart device user to perform the steps to purchase a smart device insurance product or make an insurance claim.

4. The method of claim 3, wherein the method further comprises the step of:

Providing hardware repair and replacement services, after verifying that the hardware component has not been replaced.