

APPLICATION PROCESSING METHOD AND MOBILE TERMINAL

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit and priority of Chinese Patent Application
5 No. 201210018775.2, entitled “application processing method and mobile terminal”, filed
on January 20, 2012. The entire disclosure of the application is incorporated herein by
reference.

TECHNICAL FIELD

[0002] The present disclosure relates to mobile communications, and especially to an
10 application processing method and a mobile terminal.

BACKGROUND

[0003] With the development of mobile terminals, people pay more and more
attentions to the security problem of mobile terminal applications, in which defense
against malicious fee deduction applications is an important issue of the mobile terminal
15 applications. Currently, a commonly used scheme is scan defense, the main process of
which includes: first, collecting samples of malicious fee deduction applications,
extracting their features and adding them to a virus library; when an application is to be
installed or is running, scanning the application by using an anti-virus engine, and when
the feature of the application matches a feature in the virus library (same or similar),
20 deeming the application as a virus, and prompting a user to clean it (e.g., perform
operations such as forbidding the installation, killing the virus, uninstallation, forced
uninstallation, etc.). The user can perform further processes for the application according
to the prompt, and keep the application of the mobile terminal to be safe.

[0004] The applicant finds that, at least following defects exist in the above scan
25 defense scheme: every time when an application is processed, the feature scanning needs
to be performed, which not only consumes time, but also occupies system resources, and
affects user experience of using the application.

SUMMARY

[0005] To solve the problems of time consumption and resource occupation when the security of applications is processed in existing art, embodiments of the present disclosure provide an application processing method and a mobile terminal. The technical solutions are as follows.

5 [0006] In an aspect, an application processing method is provided. The method includes:

[0007] analyzing an operation right of an application when the application executes an invoking operation for a fee deduction event;

[0008] allowing the application to execute the invoking operation if the application
10 has an operation right for the fee deduction event; and

[0009] forbidding the application from executing the invoking operation if the application does not have the operation right for the fee deduction event.

[0010] Analyzing the operation right of the application includes:

[0011] obtaining an operation permission status of the application;

15 [0012] confirming that the application has the operation right for the fee deduction event, if the operation permission status is “allowed”; and

[0013] confirming that the application does not have the operation right for the fee deduction event, if the operation permission status is “forbidden”.

[0014] Before the application executes the invoking operation for the fee deduction
20 event, the method further includes: preprocessing the application.

[0015] Preprocessing the application includes:

[0016] scanning an installation package of the application and obtaining a feature of the application; and

[0017] comparing the feature of the application with a preconfigured malicious
25 feature, and outputting prompt information of operation forbidden if the feature of the application matches the preconfigured malicious feature.

[0018] Preprocessing the application further includes:

[0019] outputting prompt information of right setting if the feature of the application does not match the preconfigured malicious feature; and

[0020] setting the operation permission status of the application according to received
5 right setting information for the application.

[0021] After preprocessing the application, the method further includes: receiving right modification information for the application, and modifying the operation permission status of the application according to the right modification information.

[0022] The operation right of the application includes any one or several of the
10 following rights: short messaging service fee deduction right, interactive voice response fee deduction right, wireless application protocol fee deduction right, wireless application protocol proxy fee deduction right, mobile payment right, and electronic bank fee deduction right.

[0023] In another aspect, a mobile terminal is also provided. The mobile terminal
15 includes:

[0024] an analysis module, configured to analyze an operation right of an application when the application executes an invoking operation for a fee deduction event; and

[0025] an execution module, configured to allow the application to execute the invoking operation if the analysis module analyzes that the application has an operation
20 right for the fee deduction event; and forbid the application from executing the invoking operation if the analysis module analyzes that the application does not have the operation right for the fee deduction event.

[0026] The analysis module includes:

[0027] an obtaining module, configured to obtain an operation permission status of
25 the application; and

[0028] an analysis module, configured to confirm that the application has the operation right for the fee deduction event, if the operation permission status is

“allowed”; and confirm that the application does not have the operation right for the fee deduction event, if the operation permission status is “forbidden”.

[0029] The mobile terminal further includes:

5 [0030] a preprocessing module, configured to preprocess the application before the application executes the invoking operation for the fee deduction event.

[0031] Specifically, the preprocessing module is configured to:

[0032] scan an installation package of the application and obtain a feature of the application; and

10 [0033] compare the feature of the application with a preconfigured malicious feature, and output prompt information of operation forbidden if the feature of the application matches the preconfigured malicious feature.

[0034] The preprocessing module is further configured to:

[0035] output prompt information of right setting if the feature of the application does not match the preconfigured malicious feature; and

15 [0036] set the operation permission status of the application according to the received right setting information for the application.

[0037] The mobile terminal further includes:

20 [0038] a modification module, configured to receive right modification information for the application and modify the operation permission status of the application according to the right modification information.

[0039] The operation right of the application includes any one or several of the following rights: short messaging service fee deduction right, interactive voice response fee deduction right, wireless application protocol fee deduction right, wireless application protocol proxy fee deduction right, mobile payment right, and electronic bank fee deduction right.

25

[0040] The advantages of the embodiments provided by the present disclosure are

that: analyzing an operation right of an application when the application executes an invoking operation for a fee deduction event; allowing the application to execute the invoking operation if the application has an operation right for the fee deduction event; and forbidding the application from executing the invoking operation if the application
5 does not have the operation right for the fee deduction event. In the embodiments of the present disclosure, when the security problem of an application is processed, it is not necessary to scan the application every time when the application runs, it is only necessary to determine the operation right of the application, which cuts down the processing time as well as saves resources, and meanwhile, it is not necessary for the user
10 to participate, which facilitates the user to use and improves the user experience.

BRIEF DESCRIPTION OF THE DRAWINGS

[0041] In order to describe the technical solutions of the embodiments of the present disclosure more clearly, a brief introduction of the accompanying drawings used to describe the embodiments will be given below. It is obvious that the attached drawings in
15 the following description only show some embodiments of the present disclosure, and other drawings can be learned by those ordinary skilled in the art without creative efforts based on these accompanying drawings.

[0042] Figure 1 shows a flowchart of an application processing method provided in Embodiment 1 of the present disclosure;

20 [0043] Figure 2 shows a flowchart of an application processing method provided in Embodiment 2 of the present disclosure;

[0044] Figure 3 shows a schematic diagram of a mobile terminal provided in Embodiment 3 of the present disclosure; and

[0045] Figure 4 shows a schematic diagram of another mobile terminal provided in
25 Embodiment 3 of the present disclosure.

DETAILED DESCRIPTION

[0046] To make the objects, technical solutions and advantages of the present disclosure clearer, the embodiments of the present disclosure will be further described in

detail with reference to the accompanying drawings.

[0047] In the embodiments of the present disclosure, short messaging service (SMS) channel fee deduction can be: a charge standard is set in a billing and service system, a mobile terminal actively sends a short message in a specific format to a specific service port, and preconfigured communication fees are deducted; interactive voice response (IVR) or voice call channel fee deduction can be: a charge standard is set in a billing and service system, a mobile terminal actively dials a service number to make a voice call, and preconfigured communication fees are deducted; wireless application protocol (WAP) channel fee deduction or WAP proxy fee deduction can be: a charge standard is set in a billing and service system, a mobile terminal connects to a specific uniform/universal resource locator (URL) via WAP, and preconfigured communication fees are deducted.

[0048] “Mobile payment” is a type of service that allows a user to use a mobile terminal to pay for bills of consumed services or products. This type of service establishes a payment account associated with a mobile terminal number of each user for each user, and provides a way of performing payment transactions and identity authentication by a mobile terminal; and “electronic bank payment” refers to a service provided by a bank to a user to use a mobile communication network and a mobile terminal to process related bank payment services, and the mobile terminal can provide a service interface.

20 [0049] Embodiment 1

[0050] As seen in Figure 1, an embodiment of the present disclosure provides an application processing method, including:

[0051] 101, analyzing an operation right of an application when the application executes an invoking operation for a fee deduction event;

25 [0052] 102, allowing the application to execute the invoking operation if the application has an operation right for the fee deduction event; and

[0053] 103, forbidding the application from executing the invoking operation if the application does not have the operation right for the fee deduction event.

[0054] In this embodiment, analyzing the operation right of the application includes:

[0055] obtaining an operation permission status of the application;

[0056] confirming that the application has the operation right for the fee deduction event, if the operation permission status of the application is “allowed”; and

5 [0057] confirming that the application does not have the operation right for the fee deduction event, if the operation permission status of the application is “forbidden”.

[0058] Optionally, before the application executes the invoking operation for the fee deduction event, the method further includes: preprocessing the application.

[0059] Advantageously, in this embodiment, preprocessing the application includes:

10 [0060] scanning an installation package of the application to obtain a feature of the application;

[0061] comparing the feature of the application with a preconfigured malicious feature; and

15 [0062] outputting prompt information of operation forbidden if the feature of the application matches the preconfigured malicious feature.

[0063] In this embodiment, preprocessing the application further includes:

[0064] outputting prompt information of right setting if the feature of the application does not match the preconfigured malicious feature; and

20 [0065] setting the operation permission status of the application for the application based on received right setting information.

[0066] Optionally, in this embodiment, after preprocessing the application, the method further includes: receiving right modification information for the application and, based on the right modification information, modifying the operation permission status of the application.

25 [0067] Optionally, in this embodiment, the operation right of the application includes

any one or several of the following rights: short messaging service (SMS) fee deduction right, interactive voice response (IVR) fee deduction right, wireless application protocol (WAP) fee deduction right, WAP proxy fee deduction right, mobile payment right, and electronic bank fee deduction right.

- 5 **[0068]** The mobile terminal in the embodiment of the present disclosure includes: cell phones, PDAs (Personal Digital Assistants), and other devices to which this embodiment is not specifically limited.

- 10 **[0069]** The beneficial effects of the method embodiment provided by the present disclosure are that: analyzing an operation right of an application when the application executes an invoking operation for a fee deduction event; allowing the application to execute the invoking operation if the application has an operation right for the fee deduction event; and forbidding the application from executing the invoking operation if the application does not have the operation right for the fee deduction event. In the embodiment of the present disclosure, when the security of an application is processed, it is not necessary to scan an application every time when the application runs, it is only necessary to determine the operation right of the application, which cuts down the processing time as well as saves resources, and meanwhile, it is unnecessary for the user to participate, which facilitates the user to use and improves the user experience.

[0070] Embodiment 2

- 20 **[0071]** See figure 2. The present embodiment provides an application processing method. The mobile terminal referred to in this embodiment can be a terminal device such as a cell phone, a PDA, etc. Using a cell phone as an example, the method specifically includes the following process.

[0072] 201, an application is preprocessed.

- 25 **[0073]** In the present embodiment, optionally, a cell phone can monitor an application and preprocess the application in the cell phone. The preprocessing process may include: scanning an installation package of the application to obtain a feature of the application; comparing the feature of the application with a preconfigured malicious feature; and outputting prompt information of operation forbidden, if the feature of the application

matches the preconfigured malicious feature. For example: when the application is ready to be installed, at first the cell phone performs preprocessing for the application. Specifically, the application can be preprocessed by using security software in the cell phone (e.g., an anti-virus engine, firewall, etc.), and if the feature of the application matches a malicious feature in a preconfigured malicious program library, then it is confirmed that the application is a malicious application and prompt information of operation forbidden is output, e.g., a prompt box “the application is a malicious program!” pops up to prompt the user to refuse to install the application; as another example, when the user downloads a certain application, at first the cell phone preprocesses an installation package of the application, and if the application is a malicious program, prompt information of download forbidden is output to prompt the user not to continue to download the application. In the embodiment, “the feature of the application matches a malicious feature” may refer to that the feature of the application is totally the same with the preconfigured malicious feature, and may also refer to that the feature of the application is similar to the preconfigured malicious feature (e.g., more than 80% or 90% of the feature is the same with the preconfigured malicious feature, and the proportion or data herein can be preconfigured as needed), and the present disclosure will not specify this.

[0074] In this embodiment, the preconfigured malicious feature can be stored in the malicious program library, and the malicious feature refers to the feature of malicious fee deduction programs. Specifically, samples of the malicious fee deduction programs can be obtained in advance, e.g., samples of various malicious fee deduction programs can be obtained from the network, and the features thereof are added to the malicious program library. Further, in the present block, preprocessing the application may further include: outputting prompt information of right setting if the feature of the application does not match the preconfigured malicious feature; and setting the operation permission status of the application based on received right setting information of the application. The operation permission status can be “allowed”, indicating that the application can perform an invoking operation for the fee deduction event; and the operation permission status can be “forbidden”, indicating that the application can’t perform the invoking operation for the fee deduction event.

[0075] The prompt information of right setting can be used to prompt the user to set

the operation permission status of the application. Specifically, every application corresponds to an operation right it may have. For example: application 1 may have a SMS fee deduction right, and application 2 may have a WAP fee deduction right; the mobile terminal can first obtain an operation right that an application may have and then
5 output prompt information of right setting to prompt the user to set the operation right that the application may have, i.e., setting an operation permission status corresponding to the operation right. For example, for the application 1, the mobile terminal outputs the prompt information of right setting to prompt the user to set the SMS fee deduction right that the application may have, and the user can set the operation permission status of the
10 SMS fee deduction right according to the prompt information. In the present embodiment, the operation right of the application includes but is not limited to any one or several of the following rights: SMS fee deduction right, IVR fee deduction right, WAP fee deduction right, WAP proxy fee deduction right, mobile payment right and electronic bank fee deduction right.

15 [0076] It is worth noting that in the embodiment, during the preprocessing process, scanning the installation package is an optional step and during the preprocessing process, scanning the installation package may not be performed and the application is installed directly, which will not be specified in the present embodiment.

[0077] 202, when the application executes the invoking operation for the fee
20 deduction event, the operation right of the application is analyzed.

[0078] In the present embodiment, since when an application is installed, the operation right of the application has already been set, and therefore when the application executes the invoking operation for the fee deduction event, first the operation right of the application is analyzed. Specifically, analyzing the operation right of the application
25 includes: obtaining the operation permission status of the application; and if the operation permission status is “allowed”, it is confirmed that the application has an operation right for the fee deduction event; if the operation permission status is “forbidden”, it is confirmed that the application does not have the operation right for the fee deduction event.

30 [0079] 203, if the application has the operation right for the fee deduction event, the

application is allowed to execute the invoking operation; and if the application does not have the operation right for the fee deduction event, the application is forbidden from executing the invoking operation.

[0080] In the present embodiment, based on the analysis result in block 202, if the application does not have the operation right for the fee deduction event, namely the operation permission status of the right is “forbidden”, and then when the application runs, it is forbidden from executing the invoking operation, namely, the application being unable to perform the fee deduction. For example, when a user installs a game application, the operation permission status of the “SMS fee deduction event” of the game application is set to be “forbidden”, then when the game program invokes a “send SMS to deduce” operation, the game program is forbidden from sending SMS, thereby avoiding related expenses.

[0081] In the present embodiment, the mobile terminal can also receive right modification information of the application. Based on the right modification information, the operation permission status of the application is modified. For example, if the user wants to modify the operation right of an application in the mobile terminal, he can send right modification information to the mobile terminal. The information may include: the modified operation permission status of the operation right; and the mobile terminal modifies the operation permission status of the application, and achieves the goal of modifying the right of the application.

[0082] The advantages provided in the method embodiment of the present disclosure are that: when an application executes an invoking operation for a fee deduction event, the operation right of the application is analyzed; if the application has an operation right for the fee deduction event, then the application is allowed to execute the invoking operation. If the application does not have an operation right for the fee deduction event, then the application is forbidden from executing the invoking operation. In the embodiment of the present disclosure, when the security problem of an application is processed, it is not necessary to scan the application every time when the application runs, it is only necessary to determine the operation right of the application, which cuts down the processing time as well as saves resources, and meanwhile, it is not necessary for the user to participate, which facilitates the user to use and improves the user experience.

And, when an application is installed, first the application is scanned, and then the invoking operation for the fee deduction event is configured accordingly, which realizes active defense of the fee deduction and can supplement the defense of malicious fee deduction programs that have not been found by scan defense.

5 **[0083] Embodiment 3**

[0084] See figure 3. The present embodiment provides a mobile terminal which includes: an analysis module 301 and an execution module 302.

[0085] The analysis module 301 analyzes the operation right of an application when the application executes an invoking operation for the fee deduction event.

10 **[0086]** The execution module 302 allows the application to execute the invoking operation if the analysis module analyzes that the application has the operation right for the fee deduction event. If the analysis module analyzes that the application does not have the operation right for the fee deduction event, then the application is forbidden from executing the invoking operation.

15 **[0087]** See figure 4. In the embodiment of the present disclosure, the analysis module 301 includes:

[0088] an obtaining unit 301a to obtain the operation permission status of the application; and

20 **[0089]** an analysis unit 301b to confirm that the application has the operation right for the fee deduction event, if the operation permission status is “allowed”; and confirm that the application does not have the operation right for the fee deduction event, if the operation permission status is “forbidden”.

[0090] See figure 4. Alternatively, the mobile terminal in the present embodiment may further include:

25 **[0091]** a preprocessing module 303, to preprocess the application prior to the application executing an invoking operation for the fee deduction event.

[0092] Advantageously, the preprocessing module 303, as described in the present

embodiment, is specifically configured to:

[0093] scan the installation package of the application and obtain a feature of the application; and

5 [0094] compare the feature of the application with a preconfigured malicious feature and, if the feature of the application matches the preconfigured malicious feature, output prompt information of operation forbidden.

[0095] Further, the preprocessing module described in the present disclosure is further configured to:

10 [0096] output prompt information of right setting if the feature of the application does not match the preconfigured malicious feature; and

[0097] set the operation permission status of the application according to received right setting information for the application.

[0098] See figure 4. Optionally, the mobile terminal in the present embodiment further includes:

15 [0099] a modification module 304, to receive the right modification information of the application and modify the operation permission status of the application according to the right modification information.

20 [00100] Optionally, in this embodiment, the operation right of the application includes any one or several of the following rights: short messaging service SMS fee deduction right, interactive voice response IVR fee deduction right, wireless application protocol WAP fee deduction right, WAP proxy fee deduction right, mobile payment right, and electronic bank fee deduction right.

25 [00101] The beneficial effects provided in this apparatus embodiment of the present disclosure are that: when an application executes an invoking operation for a fee deduction event, the operation right of the application is analyzed; if the application has an operation right for the fee deduction event, the application is allowed to execute the invoking operation; if the application does not have an operation right of the fee

deduction event, the application is forbidden from executing the invoking operation. In the embodiment of the present disclosure, when the security problem of an application is processed, it is not necessary to scan the application every time when the application runs, it is only necessary to determine the operation right of the application, which cuts down the processing time as well as saves resources, and meanwhile, it is not necessary for the user to participate, which facilitates the user to use and improves the user experience.

[00102] The mobile terminal provided in the present embodiment, specifically, and the method embodiment belong to a same idea. For detailed implementation thereof please refer to the method embodiment, which will not be elaborated herein.

10 [00103] An ordinary skilled in the art can understand that all or a part of the steps to realize the above embodiments can be carried out by hardware and can also by instructing related hardware by programs. The programs can be stored in a computer readable storage medium, and the storage medium can be a ROM, floppy disk, compact disc, etc.

15 [00104] The foregoing description of the embodiments has been provided for purpose of illustration and description. It is not intended to be exhaustive or to limit the disclosure. Any modifications, equivalent replacements, and improvements made within the spirit and principle of the present disclosure should be included in the protecting scope of the present disclosure.

WHAT IS CLAIMED IS:

1. An application processing method, comprising:
analyzing an operation right of an application when the application executes an
invoking operation for a fee deduction event;
allowing the application to execute the invoking operation if the application has an
operation right for the fee deduction event; and
forbidding the application from executing the invoking operation if the application
does not have the operation right for the fee deduction event.
2. The method according to claim 1, wherein analyzing the operation right of the
application comprises:
obtaining an operation permission status of the application;
confirming that the application has the operation right for the fee deduction event, if
the operation permission status is an allowed status; and
confirming that the application does not have the operation right for the fee deduction
event, if the operation permission status is a forbidden status.
3. The method according to claim 1, wherein before the application executes the
invoking operation for the fee deduction event, the method further comprises: preprocessing
the application.
4. The method according to claim 3, wherein preprocessing the application comprises:
scanning an installation package of the application and obtaining a feature of the
application; and
comparing the feature of the application with a preconfigured malicious feature, and
outputting prompt information of operation forbidden if the feature of the
application matches the preconfigured malicious feature.
5. The method according to claim 4, wherein preprocessing the application further
comprises:
outputting prompt information of right setting if the feature of the application does not
match the preconfigured malicious feature; and

setting the operation permission status of the application according to received right setting information for the application.

6. The method according to claim 3, wherein after preprocessing the application, the method further comprises: receiving right modification information for the application, and modifying the operation permission status of the application according to the right modification information.

7. The method according to any of claims 1 to 6, wherein the operation right of the application comprises any one or several of the following rights: short messaging service fee deduction right, interactive voice response fee deduction right, wireless application protocol fee deduction right, wireless application protocol proxy fee deduction right, mobile payment right, and electronic bank fee deduction right.

8. A mobile terminal, comprising:

an analysis module, configured to analyze an operation right of an application when the application executes an invoking operation for a fee deduction event; and
an execution module, configured to allow the application to execute the invoking operation if the analysis module analyzes that the application has an operation right for the fee deduction event; and forbid the application from executing the invoking operation if the analysis module analyzes that the application does not have the operation right for the fee deduction event.

9. The mobile terminal according to claim 8, wherein the analysis module comprises:
an obtaining module, configured to obtain an operation permission status of the application; and

an analysis module, configured to confirm that the application has the operation right for the fee deduction event, if the operation permission status is an allowed status; and confirm that the application does not have the operation right for the fee deduction event, if the operation permission status is a forbidden status.

10. The mobile terminal according to claim 8, wherein the mobile terminal further comprises:

a preprocessing module, configured to preprocess the application before the application executes the invoking operation for the fee deduction event.

11. The mobile terminal according to claim 10, wherein the preprocessing module is configured to:

scan an installation package of the application and obtain a feature of the application;
and

compare the feature of the application with a preconfigured malicious feature, and
output prompt information of operation forbidden if the feature of the application matches the preconfigured malicious feature.

12. The mobile terminal according to claim 11, wherein the preprocessing module is further configured to:

output prompt information of right setting if the feature of the application does not
match the preconfigured malicious feature; and

set the operation permission status of the application according to the received right
setting information for the application.

13. The mobile terminal according to claim 10, wherein the mobile terminal further comprises:

a modification module, configured to receive right modification information for the
application and modify the operation permission status of the application
according to the right modification information.

14. The mobile terminal according to any of claims 8-13, wherein the operation right of the application comprises any one or several of the following rights: short messaging service fee deduction right, interactive voice response fee deduction right, wireless application protocol fee deduction right, wireless application protocol proxy fee deduction right, mobile payment right, and electronic bank fee deduction right.