METHOD AND SYSTEM FOR FACILITATING TERMINAL IDENTIFIERS

BACKGROUND

Field

[0001] The present application relates to the field of computer technologies, and relates generally to a method and system for facilitating terminal identifiers to manage security among networked devices.

Related Art

[0002] A terminal identifier is a unique identifier assigned to a terminal device (e.g., a mobile phone or a computer) and used for distinguishing the terminal from other terminals. Proper equipment identification is important to network security.

[0003] Typically, when a user operates a terminal over a network, a security server may monitor and analyze user behavior such as service requests from the terminal. By analyzing the user behavior, the server can determine the strength of the association between the user and the terminal, and determine whether the user is likely to be authorized to use that terminal. The server may then take appropriate measures to manage the risk associated with the user operating the terminal. Therefore, it is important for the server to properly identify the terminal devices in the network.

[0004] Conventional approaches generally use information from a single piece of equipment of a terminal device as the identifier for the terminal. For example, one may use a media access control (MAC) address of a computer as the identifier of the computer, or an international mobile equipment identity (IMEI) of a mobile phone as the identifier for the mobile phone. However, using information from a single piece of equipment as the identifier for the terminal has a number of shortcomings. For example, access to equipment information of the terminal may be limited to those with access rights. When access to such information is limited, it may be difficult or impossible to determine the identifier for the terminal. As a result, a security server cannot identify user behavior associated with the terminal, and therefore cannot determine whether the user is an authorized user.

SUMMARY

[0004a] The invention is defined in the independent claims. Further embodiments of the invention are defined in the dependent claims.

[0005] One embodiment disclosed herein may provide a system for providing a terminal identifier to a terminal. During operation, a security server receives a registration

[0012] FIG. 1 illustrates an exemplary computing system that facilitates a terminal identifier generation process, in accordance with an embodiment of the present application.

[0013] FIG. 2 illustrates a process for providing a terminal identifier, in accordance with an embodiment of the present application.

[0014] FIG. 3 illustrates a process for acquiring a terminal identifier, in accordance with an embodiment of the present application.

[0015] FIG. 4 illustrates a process for determining a terminal identifier of a terminal when equipment information of the terminal changes, in accordance with an embodiment of the present application.

[0016] FIG. 5 illustrates a process for updating a registration information set, in accordance with an embodiment of the present application.

[0017] FIG. 6 illustrates an exemplary device for providing a terminal identifier, in accordance with an embodiment of the present application.

DETAILED DESCRIPTION OF EMBODIMENTS

[0018] Embodiments disclosed herein may provide a secure and accessible identifier for a terminal device on a network by generating a unique identifier for the terminal based on equipment information of the terminal. During operation, a security server can receive a set of registration information associated with one or more pieces of hardware or software equipment on the terminal, and then generate and assign a unique identifier to the terminal. The terminal can make this unique identifier available to other network devices for use in risk analysis, product recommendations, and other applications.

[0019] In some application scenarios, access to equipment information in a terminal may be limited. Other network devices (or other parties, network nodes, processes, objects, or other equipment) might not be able to access freely such equipment information, which is determined by the terminal's operating system or equipment manufacturer. Some conventional approaches may use the equipment information of a single equipment in the terminal as the identifier of the terminal. However, if the equipment information is not accessible, the terminal cannot be identified.

[0020] In embodiments of the present application, a security server may receive information associated with multiple pieces of equipment of a terminal. The security server may generate an identifier based on this information set, and return the identifier to the terminal. Since the terminal identifier does not depend on information of a single piece of equipment, the terminal identifier remains available even if one piece of equipment information on the terminal is inaccessible.

signed second character string), and the security server uses the third character string as the terminal identifier.

[0043] The security server, terminal, application server, and/or other network devices may use the signature of the terminal identifier to ensure the integrity of the terminal identifier (e.g., the terminal identifier has not been tampered with during the network transmission process). The devices may also use the signature to verify the authenticity of the terminal identifier (e.g., the terminal identifier has not been counterfeited by a third party). When the terminal receives the terminal identifier generated by the security server, because the terminal identifier carries a signature, the terminal may verify the authenticity and/or integrity of the terminal identifier. If the terminal can successfully verify the terminal identifier, the terminal stores and uses the terminal identifier. Likewise, after the application server acquires the terminal's signed terminal identifier, the application server may verify the authenticity and/or integrity of the terminal identifier, and subsequently provide service based upon successful verification of the terminal identifier.

[0044] If the security server is generating a terminal identifier for only one terminal, then the security server returns the terminal identifier to that terminal. However, in some scenarios, the security server may need to simultaneously generate corresponding terminal identifiers for multiple terminals. If the security server cannot determine which terminal of the multiple terminals corresponds to a registration information set I_1, the security server may not be able to return the terminal identifier generated based on the registration information set I_1 to the proper terminal. Thus, the application below describes implementation IV which may solve this collision problem. Implementation IV includes a process for generating terminal identifiers for multiple terminals and providing a proper identifier to a respective terminal.

Implementation IV - Authentication Information Set

[0045] After the security server generates the terminal identifier in operation 204, the security server may receive an authentication information set from the terminal. Similar to the registration information set, the authentication information set includes multiple pieces of equipment information. The equipment corresponding to each piece of equipment information in the authentication information set is the same as the equipment corresponding to each piece of equipment information in the registration information set. This effectively ensures that the registration information set and the authentication information set correspond to the same terminal.

[0046] The security server uses the authentication information set to determine the correct terminal identifier to return to the terminal. The security server may search for a terminal

provide the proper terminal identifier to the terminal. An embodiment which may address this problem is described below.

[0056] In one embodiment, each time the security server receives an authentication information set from the terminal and then searches for the registration information set that matches (e.g. similarity is within a predetermined threshold) and/or is most similar to the authentication information set, the security server may update the current stored registration information set.

[0057] FIG. 5 illustrates a process for updating a registration information set, in accordance with an embodiment of the present application. During operation, the security server receives an authentication information set from the terminal (operation 502). Next, the security server searches for the registration information set that matches (e.g. similarity is within a predetermined threshold) and/or is most similar to the authentication information set (operation 504). Subsequently, the security server may update the current stored registration information set (operation 506). The security server may substitute the current stored registration information set with the current received authentication information set. The security server may also store multiple versions of the registration information set. The security server may then use the authentication information set as the current updated registration information set (operation 508).

[0058] The security server may store multiple versions of the registration information set corresponding to the terminal identifier. The security server may store the original registration information set as a first registration information set, and use the current received authentication information set as a second registration information set corresponding to the same terminal identifier. Under such a scenario, the same terminal identifier may correspond to multiple registration information sets, but one registration information set only corresponds to one terminal identifier.

[0059] Thus, when the security server updates the registration information set and then receives the authentication information set of the terminal again at a predetermined time slot, the security server may search for the terminal identifier corresponding to the most recent registration information set that matches the authentication information set. Because the registration information set has been updated (e.g., either by storing multiple versions or by replacing an old registration information set), the current received authentication information set is expected to be identical to the updated registration information set, and the security server may provide the proper terminal identifier to the terminal.

[0060] While users typically change equipment such as a video card or a memory in a terminal, they do not change a large amount of equipment within a short time. The security server may substitute a registration information set with a corresponding authentication

information set received at a certain time. When a user subsequently changes the equipment in the terminal, there are only minor differences between the authentication information set of the terminal with the equipment change and the registration information set stored in the security server. Thus, the security server may still send the proper terminal identifier to the terminal, even if some equipment in the terminal has changed.

[0061] The security server may continually take the authentication information set as a new registration information set and establish a mapping relationship between the new registration information set and the terminal identifier (e.g., one terminal identifier corresponds to multiple registration information sets). Because one registration information set may only correspond to one terminal identifier, even if the equipment in the terminal changes, the security server may still find a unique matching registration information set based on the authentication information set received from the terminal with the equipment changes. The security server may return the terminal identifier corresponding to the matching registration information set to the terminal.

[0062] FIG. 6 illustrates an exemplary security server for providing a terminal identifier, in accordance with an embodiment disclosed herein. A security server 600 includes a processor 610, a memory 620, and a storage device 630. Storage 630 typically stores instructions that can be loaded into memory 620 and executed by processor 610 to perform the methods described above. In one embodiment, the instructions in storage 630 can implement a first information set acquisition module 632, a terminal identifier generating module 634, a terminal identifier sending module 636, a second information set acquisition module 638, and a terminal identifier search module 640, which can communicate with each other through various means.

[0063] In some embodiments, modules 632, 634, 636, 638 and 640 can be partially or entirely implemented in hardware and can be part of processor 610. Further, in some embodiments, security server 600 may not include a separate processor and memory. Instead, in addition to performing their specific tasks, modules 632, 634, 636, 638 and 640, either separately or in concert, may be part of special-purpose computation engines.

[0064] Storage device 630 stores programs to be executed by processor 610. Specifically, storage 630 stores a program that implements a system (e.g., application) for providing a terminal identifier. During operation, the application program can be loaded from storage 630 into memory 620 and executed by processor 610. As a result, security server 600 can perform the functions described above. Security server 600 further optionally includes a display 680, and can be coupled to a keyboard 660 and a pointing device 670, and can be coupled via one or more network interfaces to a network 682.

[0065] During operation, first information set acquisition module 632 receives a

[0070] Terminal identifier search module 640 may also be configured to search for a terminal identifier corresponding to a registration information set with similarity to the authentication information set greater than a predetermined threshold. To do so, terminal identifier search module 640 may search through a plurality of mapping relationships between each terminal identifier and a respective registration information set.

[0071] In conclusion, embodiments of the present application may reliably identify a terminal device when access to equipment information on the terminal is limited. A security server generates the identifier based on an information set which includes multiple pieces of equipment information of the terminal and serves as the registration information set, and returns the terminal identifier to the terminal. Because the terminal identifier is stored in the terminal, another device may access and acquire the terminal identifier.

[0072] Moreover, the security server may return the generated terminal identifier to the terminal at set time slots, in order to reset an expired terminal identifier or replace a lost or compromised terminal identifier. To further ensure the accuracy of the replacement terminal identifier, the security server can acquire the authentication information set again from the terminal, and determine a matching registration information set. The security server then returns to the terminal the terminal identifier corresponding to the matching registration set.

[0073] Transferring from an old terminal identifier to a new terminal identifier effectively avoids the situation in which the user behavior associated with the old terminal identifier is lost because the terminal identifier in the terminal is inaccessible. For network risk analysis, transferring to a new terminal identifier effectively avoids the situation in which malicious or illegal behavior of the user cannot be monitored because the user behavior associated with the old terminal identifier is lost, which may lead to potential financial losses. For merchants, the ability to track a user terminal identifier can avoid probable waste of marketing resources due to loss of user behavior data. Reliable identification of user terminals may solve the problem of inaccurate merchandise recommendation and invalid risk analysis.

[0074] The data structures and computer instructions described in this detailed description are typically stored on a computer-readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. The computer-readable storage medium includes, but is not limited to, volatile memory, non-volatile memory, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact discs), DVDs (digital versatile discs or digital video discs), or other media capable of storing computer-readable media now known or later developed.

[0075] The methods and processes described in the detailed description section can be embodied as code and/or data, which can be stored in a computer-readable storage medium as

What Is Claimed Is:

1. A computer-implemented method for providing a terminal identifier, comprising:

receiving, by a security server from a terminal, a registration information set comprising a first set of equipment-related information associated with a plurality of terminal equipment;

generating the terminal identifier based on the first set of equipment-related information;

receiving, from the terminal, an authentication information set comprising a second set of equipment-related information associated with the plurality of terminal equipment;

determining that a similarity between the first set of equipment-related information and the second set of equipment-related information exceeds a predetermined threshold; and

sending the terminal identifier to the terminal.

2. The method of claim 1, wherein generating the terminal identifier based on the first set of equipment-related information comprises:

generating a character string based on the first set of equipment-related information;

generating a signature based on the character string and a key of the security server;

generating the terminal identifier based on the character string and the signature, and

storing data indicating a corresponding relationship between the terminal identifier and the first set of equipment-related information.

3. The method of claim 1, wherein sending the terminal identifier to the terminal comprises:

receiving the second set of equipment-related information from the terminal;

searching for the terminal identifier corresponding to the first set of equipment-related information that matches the second set of equipment-related information from a plurality of mapping relationships between a respective terminal identifier and a respective first set of equipment-related information; and

sending the terminal identifier to the terminal.

4. The method of claim 3, wherein searching for the terminal identifier corresponding to the first set of equipment-related information that matches the second set of equipment-related information comprises:

searching for the terminal identifier corresponding to the first set of equipment-related information for which a similarity to the second set of equipment-related information is greater

than a predetermined threshold.

5. The method of claim 1, further comprising:

sending the terminal identifier to the terminal at a plurality of predetermined time slots.

6. The method of claim 1, further comprising:

receiving the second set of equipment-related information from the terminal;

updating the first set of equipment-related information currently stored with the second set of equipment-related information;

receiving a new second set of equipment-related information;

searching for the terminal identifier corresponding to the updated first set of equipment-related information that matches the new second set of equipment-related information; and

sending the terminal identifier to the terminal.

7. A device for providing a terminal identifier, comprising:

a first information set acquisition module configured to receive, by a security server from a terminal, a registration information set comprising a first set of equipment-related information associated with a plurality of terminal equipment;

a terminal identifier generating module configured to generate the terminal identifier based on the first set of equipment-related information;

a second information set acquisition module configured to receive, from the terminal, an authentication information set comprising a second set of equipment-related information associated with the plurality of terminal equipment;

the device being configured to determine that a similarity between the first set of equipment-related information and the second set of equipment-related information exceeds a predetermined threshold; and

a terminal identifier sending module configured to send the terminal identifier to the terminal.

8. The device of claim 7, wherein the terminal identifier generating module is configured to:

generate a character string based on the first set of equipment-related information;

generate a signature based on the character string and a key of the terminal identifier providing device;

generate the terminal identifier based on the character string and the signature, and

storing data indicating a corresponding relationship between the terminal identifier and the first set of equipment-related information.

9. The device of claim 7, further comprising:

the second information set acquisition module configured to receive the second set of equipment-related information from the terminal;

a terminal identifier search module configured to search for the terminal identifier corresponding to the first set of equipment-related information that matches the second set of equipment-related information from a plurality of mapping relationships between a respective terminal identifier and a respective first set of equipment-related information,

wherein the terminal identifier sending module is configured to send the terminal identifier to the terminal.

10. The device of claim 9, wherein the terminal identifier search module is configured to:

search for the terminal identifier corresponding to the first set of equipment-related information for which a similarity to the second set of equipment-related information is greater than a predetermined threshold.

11. The device of claim 7, wherein the terminal identifier sending module is further configured to send the terminal identifier to the terminal at a plurality of predetermined time slots.

12. The device of claim 7, further comprising:

the second information set acquisition module configured to receive the second set of equipment-related information from the terminal;

the terminal identifier generating module further configured to update the first set of equipment-related information currently stored with the second set of equipment-related information;

the second information set acquisition module further configured to receive a new second set of equipment-related information;

a terminal identifier search module configured to search for the terminal identifier corresponding to the updated first set of equipment-related information that matches the new

second set of equipment-related information; and

wherein the terminal identifier sending module is further configured to send the terminal identifier to the terminal.

13. A non-transitory computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for providing a terminal identifier, the method comprising:

receiving, by a security server from a terminal, a registration information set comprising a first set of equipment-related information associated with a plurality of terminal equipment;

generating the terminal identifier based on the first set of equipment-related information;

receiving, from the terminal, an authentication information set comprising a second set of equipment-related information associated with the plurality of terminal equipment;

determining that a similarity between the first set of equipment-related information and the second set of equipment-related information exceeds a predetermined threshold; and

sending the terminal identifier to the terminal.

14. The storage medium of claim 13, wherein generating the terminal identifier based on the first set of equipment-related information comprises:

generating a character string based on the first set of equipment-related information;

generating a signature based on the character string and a key of the security server; and

generating the terminal identifier based on the character string and the signature, and

storing data indicating a corresponding relationship between the terminal identifier and the first set of equipment-related information.

15. The storage medium of claim 13, wherein sending the terminal identifier to the terminal comprises:

receiving the second set of equipment-related information from the terminal;

searching for the terminal identifier corresponding to the first set of equipment-related information that matches the second set of equipment-related information from a plurality of mapping relationships between a respective terminal identifier and a respective first set of equipment-related information; and

sending the terminal identifier to the terminal.

16. The storage medium of claim 15, wherein searching for the terminal identifier

corresponding to the first set of equipment-related information that matches the second set of equipment-related information comprises:

searching for the terminal identifier corresponding to the first set of equipment-related information for which a similarity to the second set of equipment-related information is greater than a predetermined threshold.

17. The storage medium of claim 13, wherein the method further comprises:

sending the terminal identifier to the terminal at a plurality of predetermined time slots.

18. The storage medium of claim 13, wherein the method further comprises:

receiving the second set of equipment-related information from the terminal;

updating the first set of equipment-related information currently stored with the second set of equipment-related information;

receiving a new second set of equipment-related information;

searching for the terminal identifier corresponding to the updated first set of equipment-related information that matches the new second set of equipment-related information; and

sending the terminal identifier to the terminal.