

Network Authentication Method and Apparatus

The present application claims priority to Chinese Application No. 201710039832.8, filed on 19 January, 2017 and entitled “Network Authentication Method and Apparatus,” which is incorporated herein by reference in its entirety.

Technical Field

The present application relates to the technical field of network authentication, and particularly to network authentication methods and apparatuses.

Background

When a user wants to connect a user device to a wireless network, the user device is first connected to a network device such as an AP (a wireless access point), and then achieves a network access through the network device. A network access operation is actually an access operation to the Ethernet, and the network device is equivalent to a bridge between the wireless network and the Ethernet.

In related technologies, wireless networks comply with the IEEE 802.1x standard to provide access control and authentication. An enterprise scenario is used as an example. Since high information security requirements are involved, an EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) protocol such as the IEEE 802.1x standard can be used to perform network authentication on a user device that accesses a network device.

However, a PKI (Public Key Infrastructure) system needs to be deployed in an enterprise

in a process of authentication of the related technologies, and the PKI system is very large and complex, with very high initial investment and post-maintenance requirements. Furthermore, based on the deployed PKI system, a digital certificate needs to be stored individually on a user device and a server, and the validity of the digital certificate needs to be maintained periodically. Moreover, in the process of authentication, two parties need to perform mutual authentication on the digital certificate, which causes the process of authentication to be complicated and have a low efficiency.

Summary

In view of the above, the present application provides a method and an apparatus for network authentication, which can simplify a process of network authentication for a user device.

To achieve the above objectives, the present application provides the following technical solutions.

According to a first aspect of the present application, a network authentication method is provided, which includes:

receiving, by a server of a preset instant messaging application, an authentication request sent by a network device, the authentication request including a unique device identifier of a user device;

determining, by the server, an authentication result of the unique device identifier of the user device, based on a preset group having a binding relationship with the network device, a mapping relationship between identity information of associated users of the preset group

and unique device identifiers that is pre-recorded in the server, and a respective network access permission corresponding to each piece of identity information; and

returning, by the server, the authentication result to the network device, to instruct the network device to control a network access operation of the user device according to the authentication result.

According to a second aspect of the present application, a network authentication method is provided, which includes:

obtaining, by a network device client running on a network device that is bound to a preset group, a unique device identifier of a user device in response to the network device detecting an access of the user device;

sending, by the network device client, an authentication request including the unique device identifier of the user device to a server of a preset instant messaging application, wherein the authentication request is used for instructing the server to perform authentication on the unique device identifier of the user device preset based on a pre-stored mapping relationship between identity information of associated users of the preset group and unique device identifiers, and a respective network access permission corresponding to each piece of identity information; and

receiving, by the network device client, an authentication result of the unique device identifier of the user device returned by the server, and controlling a network access operation of the user device according to the authentication result.

According to a third aspect of the present application, a network authentication method is provided, which includes:

determining, by a user client of a preset instant messaging application running on an electronic device, identity information of a logged-in user; and

sending, by the user client, a notification message to a server of the instant messaging application, wherein the notification message includes the identity information and a unique device identifier of the electronic device, to cause the server to record a mapping relationship between the identity information and the electronic device, wherein the mapping relationship is used for instructing the server to apply a network access permission of the identity information in a preset group to the electronic device to control the electronic device to implement a network access operation based on network device(s) under the preset group.

According to a fourth aspect of the present application, a network authentication apparatus is provided, which includes:

a request receiving unit that causes a server of a preset instant messaging application to receive an authentication request sent by a network device, the authentication request including a unique device identifier of a user device;

an authentication unit that causes the server to determine an authentication result of the unique device identifier of the user device, based on preset groups having a binding relationship with the network device, a mapping relationship between identity information of associated users of the preset groups and unique device identifiers that is pre-recorded in the server, and a respective network access permission corresponding to each piece of identity information;

a returning unit that causes the server to return the authentication result to the network device, to instruct the network device to control a network access operation of the

user device according to the authentication result.

According to a fifth aspect of the present application, a network authentication apparatus is provided, which includes:

an acquisition unit that causes a network device client running on a network device that is bound to a preset group to obtain a unique device identifier of a user device in response to the network device detecting an access of the user device;

a sending unit that causes the network device client to send an authentication request including the unique device identifier of the user device to a server of a preset instant messaging application, wherein the authentication request is used for instructing the server to perform authentication on the unique device identifier of the user device preset based on a pre-stored mapping relationship between identity information of associated users of the preset group and unique device identifiers, and a respective network access permission corresponding to each piece of identity information; and

a control unit that causes the network device client to receive an authentication result of the unique device identifier of the user device returned by the server, and control a network access operation of the user device according to the authentication result.

According to a sixth aspect of the present application, a network authentication apparatus is provided, which includes:

a determination unit that causes a user client of a preset instant messaging application running on an electronic device to determine identity information of a logged-in user; and

a sending unit that causes the user client to send a notification message to a server of the instant messaging application, wherein the notification message includes the identity

information and a unique device identifier of the electronic device, to cause the server to record a mapping relationship between the identity information and the electronic device, wherein the mapping relationship is used for instructing the server to apply a network access permission of the identity information in a preset group to the electronic device to control the electronic device to implement a network access operation based on network device(s) under the preset group.

As can be seen from the above technical solutions, through a mapping relationship between identity information and device MAC addresses that is pre-stored on a server, the present application only needs a network device to obtain a MAC address of a user device in order to enable the server to perform authentication according to the pre-stored mapping relationship. This can not only simplify a process of authentication of the user device by the server and improve the efficiency of authentication of the user device, but can also avoid deploying a PKI system and reduce investment and complexity of an entire system.

Brief Description of the Drawings

FIG. 1 is a flowchart of a network authentication method based on a server side according to an exemplary embodiment of the present application.

FIG. 2 is a flowchart of a network authentication method based on a network device client side according to an exemplary embodiment of the present application.

FIG. 3 is a flowchart of a network authentication method based on a user client side according to an exemplary embodiment of the present application.

FIG. 4 is a schematic diagram of a scenario of an application network device according to

an exemplary embodiment of the present application.

FIG. 5 is a flowchart of a network authentication method according to an exemplary embodiment of the present application.

FIG. 6 is a flowchart of another network authentication method according to an exemplary embodiment of the present application.

FIG. 7 is a schematic structural diagram of an electronic device based on a server side according to an exemplary embodiment of the present application.

FIG. 8 is a block diagram of a network authentication apparatus based on a server side according to an exemplary embodiment of the present application.

FIG. 9 is a schematic structural diagram of an electronic device based on a network device client side according to an exemplary embodiment of the present application.

FIG. 10 is a block diagram of a network authentication apparatus based on a network device client side according to an exemplary embodiment of the present application.

FIG. 11 is a schematic structural diagram of an electronic device based on a user client side according to an exemplary embodiment of the present application.

FIG. 12 is a block diagram of a network authentication device based on a user client side according to an exemplary embodiment of the present application.

Detailed Description

FIG. 1 is a flowchart of a network authentication method based on a server side according to an exemplary embodiment of the present application. As shown in FIG. 1, the method is applied to a server, and may include the following steps.

Step 102: A server of a preset mobile enterprise work platform receives an authentication request sent by a network device, the authentication request including a unique device identifier of a user device.

In the present embodiment, a mobile enterprise work platform can not only realize a communication function, but can also be used as an integrated function platform for a number of other functions. Examples include processing internal events of an enterprise, such as examination and approval events (such as leave, office item application, financial and other examination and approval events), attendance events, task events, log events, etc., and processing of external events, such as ordering and purchasing, which are not limited in the present application.

More specifically, mobile enterprise work platforms can be hosted in instant messaging applications in related technologies, for example, enterprise instant messaging (EIM) applications, such as Skype For Business®, Microsoft Teams®, Yammer®, Workplace®, Slack®, Enterprise WeChat®, Fxiaoke®, Enterprise Feixin®, Enterprise Yixin®, etc. Apparently, an instant messaging function is only one of a number of communication functions supported by the mobile enterprise work platform. The enterprise work platform can also implement more such as other functions as described above, which are not redundantly described herein.

In the present embodiment, a unique device identifier can uniquely indicate and determine a corresponding user device, i.e., the unique device identifier has a one-to-one correspondence relationship with the user device. All pieces of identification information having a property of uniqueness can be used as a unique device identifier, which is not limited

in the present application. For example, the unique device identifier may be a MAC (Media Access Control) address, a serial number of the user device, etc.

Step 104: The server determines an authentication result of the unique device identifier of the user device, based on a preset group having a binding relationship with the network device, a pre-recorded mapping relationship between identity information of associated users of the preset group and unique device identifiers in the server, and a respective network access permission corresponding to each piece of identity information.

In the present embodiment, since the network device can only cover a certain range near a location of installation thereof (i.e., only user devices within that range can access the network device), the network device is usually bound to a preset group, and is installed within a working range of the preset group(s), so that associated users of the preset group can access and perform network access operations. A “group” may refer to various organizations such as enterprises, schools, hospitals, military units, and government agencies. These forms of organizations can adopt the above-mentioned mobile enterprise work platform to implement the technical solutions of the present application.

In the present embodiment, the server pre-records a mapping relationship between each associated user of the preset group and a corresponding unique device identifier, so as to perform authentication on the unique device identifier of the user device sent by the network device according to the recorded mapping relationship at a later time. When receiving a notification message sent by an electronic device, the server records a corresponding mapping relationship between identity information logged in a user client of the mobile enterprise work platform running on the electronic device and a unique device identifier of the electronic device

included in the notification message based on the identity information and the unique device identifier included in the notification message. Apparently, in other cases, a management user of the preset group may also create such mapping relationship manually, or may edit a mapping relationship that is already recorded in the server.

In the present embodiment, an associated user of the preset group may include at least one of the following: an internal member of the preset group, an external contact of the preset group (such as an internal member of another group that has an association relationship with the preset group, e.g., such other group and the preset group have a cooperative relationship), an external visitor of the preset group, etc. Apparently, other types of associated users may also be adapted to the technical solutions of the present application, which are not limited in the present application.

In the present embodiment, since multiple associated users can perform account logins using a same user device, and a same associated user can also perform an account login on multiple user devices, the server may have multiple mapping relationships corresponding to a unique device identifier of such user device at the same time. As such, the server may select a most recently recorded mapping relationship to determine an authentication result corresponding to the unique device identifier of the user device. In practice, when detecting a login activity or an access instruction to the network device from a user, the user device may send a notification message as described above to the server, so that the server updates a mapping relationship corresponding to the user device, thereby ensuring that the mapping relationship used for authentication corresponds to an associated user who is currently logged

onto the user device, and avoids applying network access permission corresponding to other associated users for authentication.

Step 106: The server returns the authentication result to the network device, to instruct the network device to control a network access operation of the user device according to the authentication result.

Correspondingly, FIG. 2 is a flowchart of a network authentication method based on a network device client side according to an exemplary embodiment of the present application. As shown in FIG. 2, the method is applied to a network device client, and may include the following steps.

Step 202: A network device client running on a network device obtains a unique device identifier of a user device when the network device bound to a preset group detects an access from the user device.

In the present embodiment, the network device client may be a client based on a mobile enterprise work platform, or may be other client of any form, as long as the client can cooperate with a server to perform authentication and network access control on the user device, which is not limited by the present application. Apparently, when the network device client is a client based on a mobile enterprise work platform, the network device client has a built-in control logic cooperated with the server, which makes implementing the technical solutions based on the present application more easily.

In the present embodiment, the network device may include any electronic device that implements a network access function, such as an AP device, which is not limited by the present application.

Step 204: The network device client sends an authentication request that includes the unique device identifier of the user device to a server of a preset mobile enterprise work platform, wherein the authentication request is used for instructing the server to perform authentication on the unique device identifier of the user device based on a pre-stored mapping relationship between respective identity information of associated users of the preset group and unique device identifiers, and network access permission corresponding to each piece of identity information.

Step 206: The network device client receives an authentication result of the unique device identifier of the user device returned by the server, and controls a network access operation of the user device according to the authentication result.

In the present embodiment, the network device client may control a network access operation according to a value of a permission option included in the authentication result. The permission option may include at least one of the following:

1) Is authorized? If authorized, a network access can be opened directly, or a further access control can be performed in combination with other permission options; if not authorized, the network access can be denied directly.

2) A valid period of permission: For example, when an associated user is a visitor, he/she is restricted to have network accesses within the same day only. If the valid period of permission is not past, a network access can be opened directly, or a further access control can be performed in combination with other permission options; if the valid period of permission is past, the network access can be denied directly.

3) A number of remaining usages of permission: For example, for a network permission of an temporary application, the number of remaining usages of permission may be limited to one, i.e., the user can access the network device and achieve a network access only once. After the associated user accesses the network device and implements network access, a corresponding number of remaining usages of permission is decremented by one to manage the number of remaining usages of permission. Then, when the number of remaining usages of permission is not zero, a network access can be directly opened, or a further access control can be performed in combination with other permission options. When the number of remaining usages of permission is zero, the network access can be directly denied.

4) A network range that is allowed to access: A network can be pre-divided into multiple ranges, such as an internal network of the preset group, a public network outside the preset group, a domestic range in the public network, and a foreign range in the public network, thereby performing a more detailed permission control for network access operations, which is not described exhaustively herein.

Correspondingly, FIG. 3 is a flowchart of a network authentication method based on a user client side according to an exemplary embodiment of the present application. As shown in FIG. 3, the method is applied to a user client, and may include the following steps.

Step 302: A user client of a preset mobile enterprise work platform running on an electronic device determines identity information of a logged-in user.

In the present embodiment, an application program of a client of a mobile enterprise work platform can be pre-installed on an electronic device, such that the client can be launched and run on the electronic device. Apparently, when an online “client” such as HTML5

technology is used, the client can be obtained and run without the need of installing a corresponding application on the electronic device. When the network device client is a client of a mobile enterprise work platform, the above description also applies here, and details thereof are not described herein again.

Step 304: The user client sends a notification message to a server of the mobile enterprise work platform, where the notification message includes identity information and a unique device identifier of the electronic device, and a mapping relationship between the identity information and the electronic device is to be recorded by the server.

In the present embodiment, a mapping relationship recorded by the server corresponds to mapping relationships of the embodiments shown in FIG. 1 and FIG. 2. The mapping relationship is used for instructing the server to apply a network access permission of the identity information in a preset group to the electronic device (the electronic device can be determined based on the unique device identifier recorded in the mapping relationship), to control a network access operation performed by the electronic device based on network device(s) under the preset group.

In an embodiment, the electronic device may send a notification message as described above when the user client detects a user login activity. In this case, as long as a user account that is logged in on the electronic device changes, a mapping relationship recorded by the server may be updated according to a correspondence relationship between identity information corresponding to a currently logged-in user account and the unique device identifier of the electronic device, thereby ensuring that the server can perform authentication on the electronic device using the latest mapping relationship.

In another embodiment, the electronic device may send a notification message as described above when the user client detects an access instruction for any network device. In this case, when an account change occurs when the electronic device is not connected to the network device, a notification message may be sent when an access instruction is detected even if no notification message has been sent when a user login activity occurs. As such, the server updated a recorded mapping relationship in time to ensure that authentication is performed on the electronic device using the latest mapping relationship.

As can be seen from the above technical solutions, by pre-storing a mapping relationship between identity information and device MAC addresses in a server, a network device only needs to obtain a MAC address of a user device, and the server can perform authentication according to the pre-stored mapping relationship. This can not only simplify a process of authentication of the user device by the server and improve the efficiency of authentication of the user device, but can also avoid deploying a PKI system and reduce investment and complexity of an entire system.

FIG. 4 is a schematic diagram of a scenario of an application network device according to an exemplary embodiment of the present application. As shown in FIG. 4, an AP device 41 as a network device is assumed to be installed at a point A in an office area 42 of an enterprise AA, and an AP device 41 can transmit a Beacon (beacon) frame signal within a range 40 (with the point A as the center and an emission radius d as a radius of the range), so that an electronic device in the range 40 can access the AP device 41 by scanning the Beacon frame signal. Apparently, the electronic device can adopt a way of active scanning to implement scanning and accessing to the AP device 41, which is not limited by the present application. For example,

when a user is located at a point B within the range 40, a mobile phone 43 used by the user can scan and access the AP device 41, and the mobile phone 43 and the AP device 41 can implement data interactions with a server 44 respectively, thereby implementing the network authentication solutions of the present application.

The server 44 may be a physical server including an independent host. Alternatively, the server 44 may be a virtual server hosted by a host cluster. Alternatively, the server 44 may be a cloud server. During operations, the server 44 can run a server-side program of a certain application to implement associated service functions of the application, such as a network authentication function.

The mobile phone 43 is just one type of electronic device that can be used by a user. In fact, the user can apparently also use electronic devices such as tablet devices, notebook computers, PDAs (Personal Digital Assistants), wearable devices (such as smart glasses, smart watches, etc.), etc., which are not limited by the present application. During operations, the electronic device can run a client-side program of a certain application to implement associated service functions of the application, such as a network authentication function as described above.

A network in which the mobile phone 43 (or the AP device 41) conducts interactions with the server 44 may include various types of wired or wireless networks. In an embodiment, the network may include a Public Switched Telephone Network (PSTN) and the Internet.

For the sake of understanding, an enterprise instant messaging application “enterprise WeChat” is used as an example. The mobile phone 43 and the AP device 41 are assumed to run an enterprise WeChat client respectively, and an enterprise WeChat server is run on the

server 44. The enterprise WeChat client is logged in with a registered account of a user on the mobile phone 43, i.e., the mobile phone 43 is configured with an enterprise WeChat client of the user. With reference to FIGS. 5-6, the technical solutions of the present application are described in detail hereinafter using a process of performing a network access by the mobile phone 43 to access the AP device 41 as an example. FIG. 5 is a flowchart of a network authentication method provided by an exemplary embodiment of the present application. As shown in FIG. 5, the method may include the following steps.

Step 502: The mobile phone 43 detects a user login activity.

In the present embodiment, when a user login activity occurs, a change in user account may occur. Therefore, the enterprise WeChat client running on the mobile phone 43 may monitor user login activities and send a notification message as described below accordingly, to ensure a timely update of a mapping relationship recorded on the enterprise WeChat server running on the server 44.

Step 504: The mobile phone 43 sends a notification message to the server 44, where the notification message includes identity information of a logged-in account and a MAC address of the mobile phone 43.

In the present embodiment, the enterprise WeChat client running on the mobile phone 43 obtains identity information of a logged-in account, and generates a notification message including the identity information. At the same time, the notification message itself includes a MAC address of the mobile phone 43 (i.e., a source MAC address), and thus the notification message includes both the identity information of the logged-in account and the

MAC address of the mobile phone 43 without the need for the enterprise WeChat client to actively add the MAC address to the notification message.

Step 506: The server 44 records a corresponding mapping relationship according to the identity information and the MAC address included in the notification message.

In the present embodiment, if a mapping relationship between the identity information and the MAC address included in the notification message has not been recorded in the server 44, the server 44 may create such mapping relationship. If the mapping relationship between the identity information and the MAC address included in the notification message has been recorded in the server 44, the server 44 can update a recording time of this mapping relationship.

In the present embodiment, a same user account can be logged in on multiple electronic devices individually. Therefore, for the identity information included in the notification message, the server 44 can separately record respective mapping relationships between the identity information and multiple MAC addresses. Similarly, different user accounts can be separately logged in on a same electronic device. Therefore, for the MAC address included in the notification message, the server 44 can separately record respective mapping relationships between the MAC address and a plurality of pieces of identity information.

It should be noted that the above steps 502-506 describe a process of recording a mapping relationship by the server 44, and this process may occur at any arbitrary time before step 512 (to ensure that this mapping relationship can be used for an operation of authentication at step 512). Such arbitrary time is determined based on a time of detecting the user login activity at step 502 in the embodiment as shown in FIG. 5.

Step 508: A WIFI connection is established between the mobile phone 43 and the AP device 41.

In the present embodiment, the mobile phone 43 can scan and detect the AP device 41 by means of active scanning or passive scanning, and access the AP device 41 based on an access instruction, so that a WIFI connection is established between the mobile phone 43 and the AP device 41.

The access instruction may be initiated by the user of the mobile phone 43. For example, the mobile phone 43 may display all AP devices that are scanned and found. When the user selects the AP device 41, the mobile phone 43 may determine that the mobile device 43 receives an access instruction for the AP device 41. The access instruction may also be automatically generated by the mobile phone 43. For example, in the previous process of accessing the AP device 41, an access operation is set to an “automatic access” mode. As such, when the mobile phone 43 subsequently scans and finds the AP device 41 without accessing other AP devices, the mobile phone 43 will automatically generate or determine that an access instruction has been generated, and automatically access the AP device 41.

Step 510: The AP device 41 obtains the MAC address of the mobile phone 43, and sends an authentication request for the MAC address to the server 44.

Step 512: The server 44 performs authentication on the mobile phone 43 according to a recorded mapping relationship.

In the present embodiment, the AP device 41 is assumed to have been bounded to the enterprise AA in advance. For example, a management user of the enterprise AA performs a binding of the AP device 41 on the enterprise WeChat, and thus the server 44 has a record of a

binding relationship between the AP device 41 and the enterprise AA. Furthermore, the server 44 also has records of: mapping relationships corresponding to all associated users of the enterprise AA, and a respective network access permission of each associated user.

In one case, it is assumed that, after the server 44 receives the MAC address of the mobile phone 43, a mapping relationship that matches with the MAC address is not found, or identity information in a mapping relationship that matches with the MAC address is not an associated user of the enterprise AA. In this case, the server 44 can determine that the mobile phone 43 does not have a network access permission, i.e., an authentication result is that the authentication fails.

In another case, it is assumed that, after the server 44 receives the MAC address of the mobile phone 43, a mapping relationship that matches with the MAC address is found, and identity information recorded in the mapping relationship belongs to an associated user of the enterprise AA. As such:

If network access permissions of all associated users of the enterprise AA are the same, the server 44 can determine that the mobile phone 43 has passed the authentication and return a corresponding authentication result to the AP device 41, to cause the AP device 41 to open a network access permission of the mobile phone 43, for example, allowing the mobile phone 43 to access an external public network from within the enterprise AA.

If network access permissions of various types of associated users in the enterprise AA are different (for example, when the associated users in the enterprise AA include multiple types, such as internal members, external contacts, and external visitors, etc.), an associated user type to which identity information belongs can further be determined based on the

identity information, the identity information being recorded in a mapping relationship that matches with the MAC address of the mobile phone 43. A corresponding authentication result is then returned to the AP device 41 according to a network access permission corresponding to the associated user type, so that the AP device 41 can control a network access operation of the mobile phone 43 according to the authentication result. Apparently, associated users of a same type can be further divided into multiple sub-types, such as further dividing the internal members into a management type, a research and development type, a sales type, etc. Furthermore, associated users of each sub-type can have corresponding network access permissions, and the server 44 can also send corresponding authentication results according thereto. Details thereof are not described herein again.

In the present embodiment, the server 44 may only find a mapping relationship that matches with the MAC address of the mobile phone 43. The server 44 may directly perform authentication on the mobile phone 43 according to identity information of an associated user recorded in the mapping relationship. The server 44 may also find a plurality of mapping relationships matching with the MAC addresses of the mobile phone 43 at the same time. In this case, the server 44 may select the most recently recorded mapping relationship to perform authentication on the mobile phone 43.

The most recently recorded mapping relationship, i.e., a mapping relationship having the last editing time that is the latest. The last editing time may be a time of creation or a time of update. If the server 44 receives a notification message including identity information 1 and a MAC address 1, and creates a mapping relationship 1 between the identity information 1 and the MAC address 1 at time 1, the last editing time for the mapping relationship 1 is a time of

creation, i.e., time 1. When the server 44 receives a notification message including the identity information 1 and the MAC address 1 again, the server 44 may update the last editing time of the mapping relationship 1 at time 2, and the last editing time is then changed from a time of creation to a time of update (i.e., the time at which an update operation is performed), i.e., time 2. Similarly, when the server 44 receives a notification message including the identity information 1 and the MAC address 1 again, the server 44 may update the last editing time of the mapping relationship 1 at time 3. In this case, the last editing time is changed from time 2 to a time of update (i.e., the time at which an update operation is performed), i.e., time 3.

Step 514: The server 44 sends an authentication result to the AP device 41.

Step 516: The AP device 41 performs a permission control on the mobile phone 43 according to the authentication result to manage a network access operation thereof.

In the present embodiment, the authentication result may include a number of permission options, and the AP device 41 may control a network access operation of the mobile phone 43 according to respective value(s) of the permission option(s). The permission option(s) include(s) at least one of the following: whether is authorized, a valid period of permission, a number of remaining usages of permission, a network range allowed to access. Apparently, more types of permission options may be used, and the present application does not have any limitations thereon.

In a relatively simple logic of permission management, the authentication result may include only “whether is authorized”. For example, a value of one means that it is authorized, and a value of zero means that it is not authorized. Therefore, the AP device 41 allows the

mobile phone 43 to perform a full network access operation when the value is one, and denies the mobile phone 43 to perform any network access operation when the value is zero.

In a more complex logic of permission management, the authentication result can contain multiple permission options at the same time. For example:

When the authentication result includes both “whether it is authorized” and “network range allowed to access”, if a value of “whether it is authorized” indicates that it is authorized, and a value of “network range allowed to access” indicates an internal local area network and an external public network, the mobile phone 43 is allowed to perform network access operations on the internal local area network and the external public network. If the value of “whether it is authorized” indicates that it is authorized, and the value of “network range allowed to access” indicates an internal local area network, the mobile phone 43 is allowed to perform network access operations on the internal local area network, and is restricted from accessing the external public network. If the value of “whether it is authorized” indicates that it is not authorized, the mobile phone 43 is denied from performing any network access operations regardless what the value of “network range allowed to access” is. Other situations are not redundantly described herein.

When the authentication result includes “whether it is authorized”, “valid period of permission”, and “network range allowed to access”, if a value of “whether it is authorized” indicates that it is authorized, a value of “valid period of permission” indicates that it is not expired, and a value of “network range allowed to access” indicates an internal local area network and an external public network, the mobile phone 43 is allowed to perform network access operations on the internal local area network and the external public network. If the

value of “whether it is authorized” indicates that it is authorized and the value of “valid period of permission” indicates that it is expired, the mobile phone 43 is denied from performing any network access operations regardless of what the value of “network range allowed to access” is. Other situations are not redundantly described herein.

Apparently, different modes of permission management can be implemented using a combination of any of a plurality of permission options, in order to satisfy permission management requirements in different scenarios, which are not exhaustively described herein, and are not limited by the present application.

In the embodiment shown in FIG. 5, the mobile phone 43 may send a notification message to the server 44 by using a “detected user login activity” as a triggering condition, so that the server 44 can create or update a mapping relationship corresponding to the mobile phone 43. If the user account is logged in on the mobile phone 43 for the first time (logging in on the mobile phone 43 for the first time, but may have been logged in on other electronic devices), the server 44 needs to create a corresponding mapping relationship, if the user account is not logged in on the mobile phone 43 for the first time (a login operation has previously been performed on the mobile phone 43), the server 44 needs to update a corresponding mapping relationship (such as updating the last editing time thereof).

In practice, the mobile phone 43 can also send a notification message as described above to the server 44 based on other conditions, to ensure that a mapping relationship recorded on the server 44 remains updated. For example, as shown in FIG. 6, in a network authentication method of another exemplary embodiment, the method may include the following steps.

Step 602: The mobile phone 43 scans and finds the AP device 41.

In the present embodiment, the mobile phone 43 can scan and find the AP device 41 by means of active scanning or passive scanning, which is not limited in the present application.

Step 604: The mobile phone 43 detects an access instruction.

In the present embodiment, the access instruction may be initiated by a user of the mobile phone 43. For example, the mobile phone 43 may show all AP devices that are scanned and found. When the user selects the AP device 41, the mobile phone 43 may determine that the mobile phone 43 receives an access instruction for the AP device 41. The access instruction may also be automatically generated by the mobile phone 43. For example, in a previous process of accessing the AP device 41, an access operation is set to be an “automatic access” mode. In this case, when the mobile phone 43 scans and finds the AP device 41 in a subsequent process and has not accessed other AP devices yet, the mobile phone 43 will automatically generate or determine that an access instruction has been generated and automatically access the AP device 41.

Step 606: The mobile phone 43 sends a notification message to the server 44, the notification message including identity information of a logged-in account and a MAC address of the mobile phone 43.

In the present embodiment, since it is desired to have the AP device 41 to manage permissions of the mobile phone 43 about network accesses in the present application, if no access instruction is detected when a login of a user account occurs in the mobile phone 43, this indicates that the AP device 41 is not involved in permission management of the mobile phone 43. In this case, the mobile phone 43 does not need to send a notification message to

the server 44. When the mobile phone 43 detects an access instruction, the server 44 can promptly create or update a mapping relationship corresponding to the mobile phone 43 by sending a notification message to the server 44, to ensure that the mapping relationship recorded on the server 44 is the latest data.

For subsequent steps 608-618, reference may be made to steps 506-516 in the embodiment as shown in FIG. 5, and details thereof are not described herein again.

In short, based on a mobile enterprise work platform, the present application can have a mapping relationship between identity information and a device MAC address to be recorded on a server of the mobile enterprise work platform, and an authentication on a network access permission of a user device can be quickly performed according to the mapping relationship, thus effectively simplifying the complexity of a process of authentication and ensures the efficiency of authentication while ensuring the security of network data.

FIG. 7 shows a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 7, at a hardware level, the electronic device includes a processor 702, an internal bus 704, a network interface 706, a memory 708, and a non-volatile memory 710. Apparently, hardware components needed by other services may also be included. The processor 702 reads a corresponding computer program from the non-volatile memory 710 into the memory 702 and then operates to form a network authentication apparatus at a logical level. Apparently, in addition to software implementations, the present application does not exclude other manners of implementation, such as a logic device or a combination of software and hardware, etc. In other words, an

execution body of the following flow of processing is not limited to various logical units, and may be hardware or logic device(s).

Referring to FIG. 8, in a software implementation, the network authentication apparatus may include a request receiving unit 801, an authentication unit 802, and a returning unit 803.

The request receiving unit 801 causes a server of a preset mobile enterprise work platform to receive an authentication request sent by a network device, the authentication request including a unique device identifier of a user device.

The authentication unit 802 causes the server to determine an authentication result of the unique device identifier of the user device, based on a preset group having a binding relationship with the network device, a mapping relationship between identity information of associated user(s) of the preset group and unique device identifier(s) that is pre-recorded in the server, and a respective network access permission corresponding to each piece of identity information.

The returning unit 803 causes the server to return the authentication result to the network device, to instruct the network device to control a network access operation of the user device according to the authentication result.

Optionally, the apparatus also includes:

a message receiving unit 804 that causes the server to receive a notification message sent by an electronic device, the notification message including identity information that is logged in a user client of the mobile enterprise work platform running on the electronic device, and a unique device identifier of the electronic device; and

a recording unit 805 that causes the server to record the identity information and the unique device identifier included in the notification message as a corresponding mapping relationship.

Optionally, the apparatus also includes:

a selection unit 806 that causes the server to select a most recently recorded mapping relationship for determining the authentication result corresponding to the unique device identifier of the user device when multiple mapping relationships corresponding to the unique device identifier of the user device exist.

Optionally, the associated user(s) include(s) at least one of the following: an internal member of the preset group, an external contact of the preset group, and an external visitor of the preset group.

FIG. 9 shows a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 9, at a hardware level, the electronic device includes a processor 902, an internal bus 904, a network interface 906, a memory 908, and a non-volatile memory 910. Apparently, hardware components needed by other services may also be included. The processor 902 reads a corresponding computer program from the non-volatile memory 910 into the memory 908 and then operates to form a network authentication apparatus at a logical level. Apparently, in addition to software implementations, the present application does not exclude other manners of implementation, such as a logic device or a combination of software and hardware, etc. In other words, an execution body of the following flow of processing is not limited to various logical units, and may be hardware or logic device(s).

Referring to FIG. 10, in a software implementation, the network authentication apparatus may include an acquisition unit 1001, a sending unit 1002, and a control unit 1003.

The acquisition unit 1001 causes a network device client running on a network device that is bound to a preset group to obtain a unique device identifier of a user device in response to the network device detecting an access of the user device.

The sending unit 1002 causes the network device client to send an authentication request including the unique device identifier of the user device to a server of a preset mobile enterprise work platform, wherein the authentication request is used for instructing the server to perform authentication on the unique device identifier of the user device preset based on a pre-stored mapping relationship between identity information of associated users of the preset group and unique device identifiers, and a respective network access permission corresponding to each piece of identity information.

The control unit 1003 causes the network device client to receive an authentication result of the unique device identifier of the user device returned by the server, and control a network access operation of the user device according to the authentication result.

Optionally, the control unit 1003 is specifically configured to:

cause the network device client to control the network access operation according to a value of a permission option included in the authentication result, wherein the permission option includes at least one of the following: whether the permission exists, a valid period of the permission, and a number of remaining usages of the permission, and a network range allowed to access.

FIG. 11 shows a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 11, at a hardware level, the electronic device includes a processor 1102, an internal bus 1104, a network interface 1106, a memory 1108, and a non-volatile memory 1110. Apparently, hardware components needed by other services may also be included. The processor 1102 reads a corresponding computer program from the non-volatile memory 1110 into the memory 1108 and then operates to form a network authentication apparatus at a logical level. Apparently, in addition to software implementations, the present application does not exclude other manners of implementation, such as a logic device or a combination of software and hardware, etc. In other words, an execution body of the following flow of processing is not limited to various logical units, and may be hardware or logic device(s).

Referring to FIG. 12, in a software implementation, the network authentication apparatus may include a determination unit 1201 and a sending unit 1202.

The determination unit 1201 causes a user client of a preset mobile enterprise work platform running on an electronic device to determine identity information of a logged-in user.

The sending unit 1202 causes the user client to send a notification message to a server of the mobile enterprise work platform, wherein the notification message includes the identity information and a unique device identifier of the electronic device, to cause the server to record a mapping relationship between the identity information and the electronic device, wherein the mapping relationship is used for instructing the server to apply a network access permission of the identity information in a preset group to the electronic device to control the electronic device to implement a network access operation based on network device(s) under

the preset group.

Optionally, the sending unit 1202 causes the user client to send the notification message to the server of the mobile enterprise work platform using at least one of the following ways:

sending the notification message when the user client detects a user login activity; and

sending the notification message when the user client detects an access instruction for any network device.

The systems, apparatuses, modules or units illustrated in the foregoing embodiments may be implemented by a computer chip or an entity, or by a product having certain functions. A typical implementation device is a computer, and a specific form of the computer may be a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email transceiver, and a game control, a tablet, a tablet, a wearable device, or a combination of any of these devices.

In a typical configuration, a computer includes one or more processors (CPUs), an input/output interface, a network interface, and memory.

The memory may include a form of computer readable media such as a volatile memory, a random access memory (RAM) and/or a non-volatile memory, for example, a read-only memory (ROM) or a flash RAM. The memory is an example of a computer readable media.

The computer readable media may include a volatile or non-volatile type, a removable or non-removable media, which may achieve storage of information using any method or technology. The information may include a computer-readable instruction, a data structure, a program module or other data. Examples of computer storage media include, but not limited to, phase-change memory (PRAM), static random access memory (SRAM), dynamic random access

memory (DRAM), other types of random-access memory (RAM), read-only memory (ROM), electronically erasable programmable read-only memory (EEPROM), quick flash memory or other internal storage technology, compact disk read-only memory (CD-ROM), digital versatile disc (DVD) or other optical storage, magnetic cassette tape, magnetic disk storage or other magnetic storage devices, or any other non-transmission media, which may be used to store information that may be accessed by a computing device. As defined herein, the computer readable media does not include transitory media, such as modulated data signals and carrier waves.

It also needs to be understood that terms “including”, “containing” or any other variations are intended to encompass a non-exclusive inclusion, such that a process, method, product, or device including a series of elements includes not only these elements, but also other elements that are not explicitly listed, or elements that are inherent to such process, method, product, or device. With any further limitation, an element defined by a phrase “comprising a ...” does not exclude the presence of additional equivalent elements in the process, method, product, or device including such element.

Exemplary embodiments are described in detail herein, examples of which are illustrated in the accompanying drawings. When accompanying drawings are involved in the following description, the same numerals in different drawings represent the same or similar elements unless indicated otherwise. The implementations described in the following exemplary embodiments do not represent all available embodiments that are consistent with the present application. Rather, they are merely examples of apparatuses and methods that are

consistent with some aspects of the present application as described in detail in the appended claims.

Terminologies used in the present application are merely intended to describe particular embodiments, and are not intended to be limiting. Singular forms “a”, “the” and “said” are intended to include a plural form, unless other meanings are clearly represented in the context. It should also be understood that a term “and/or” as used herein refers to and encompasses any and all possible combinations of one or more of associated items that are listed.

It should be understood that, although the present application may use terms such as “first”, “second”, “third”, etc. to describe various types of information, these pieces of information should not be limited to these terms. These terms are only used for distinguishing information of a same type from each other. For example, first information may also be referred to as second information without departing from the scope of the present application. Similarly, second information may also be referred to as first information. Depending on the context, a term “if” as used herein may be interpreted as “at the time of” or “when” or “in response to determining that”.

The above description is only preferred embodiments of the present application, and is not intended to limit the present application. Any modifications, equivalent replacements, improvements, etc., that are made within the spirit and principles of the present application, shall be included in the scope of protection of the present application.

Claims

1. A network authentication method comprising:

receiving, by a server of a preset instant messaging application, an authentication request sent by a network device, the authentication request including a unique device identifier of a user device;

determining, by the server, an authentication result of the unique device identifier of the user device, based on a preset group having a binding relationship with the network device, a mapping relationship between identity information of associated users of the preset group and unique device identifiers that is pre-recorded in the server, and a respective network access permission corresponding to each piece of identity information; and

returning, by the server, the authentication result to the network device, to instruct the network device to control a network access operation of the user device according to the authentication result.

2. The method of claim 1, further comprising:

receiving, by the server, a notification message sent by an electronic device, the notification message including identity information that is logged in a user client of the instant messaging application running on the electronic device, and a unique device identifier of the electronic device; and

recording, by the server, the identity information and the unique device identifier included in the notification message as a corresponding mapping relationship.

3. The method of claim 1, further comprising:

selecting, by the server, a most recently recorded mapping relationship for determining the authentication result corresponding to the unique device identifier of the user device when multiple mapping relationships corresponding to the unique device identifier of the user device exist.

4. The method of claim 1, wherein the associated users comprise at least one of the following: an internal member of the preset group, an external contact of the preset group, and an external visitor of the preset group.

5. A network authentication method comprising:

obtaining, by a network device client running on a network device that is bound to a preset group, a unique device identifier of a user device in response to the network device detecting an access of the user device;

sending, by the network device client, an authentication request including the unique device identifier of the user device to a server of a preset instant messaging application, wherein the authentication request is used for instructing the server to perform authentication on the unique device identifier of the user device preset based on a pre-stored mapping relationship between identity information of associated users of the preset group and unique device identifiers, and a respective network access permission corresponding to each piece of identity information; and

receiving, by the network device client, an authentication result of the unique device

identifier of the user device returned by the server, and controlling a network access operation of the user device according to the authentication result.

6. The method of claim 5, wherein controlling the network access operation of the user device according to the authentication result comprises:

controlling, by the network device client, the network access operation according to a value of a permission option included in the authentication result, wherein the permission option includes at least one of the following: whether the permission exists, a valid period of the permission, and a number of remaining usages of the permission, and a network range allowed to access.

7. A network authentication method comprising:

determining, by a user client of a preset instant messaging application running on an electronic device, identity information of a logged-in user; and

sending, by the user client, a notification message to a server of the instant messaging application, wherein the notification message includes the identity information and a unique device identifier of the electronic device, to cause the server to record a mapping relationship between the identity information and the electronic device, wherein the mapping relationship is used for instructing the server to apply a network access permission of the identity information in a preset group to the electronic device to control the electronic device to implement a network access operation based on a network device under the preset group.

8. The method of claim 7, wherein sending, by the user client, the notification message to the server of the instant messaging application comprises at least one of the following:

 sending the notification message when the user client detects a user login activity; and
 sending the notification message when the user client detects an access instruction for any network device.

9. A network authentication apparatus comprising:
 a request receiving unit that causes a server of a preset instant messaging application to receive an authentication request sent by a network device, the authentication request including a unique device identifier of a user device;

 an authentication unit that causes the server to determine an authentication result of the unique device identifier of the user device, based on a preset group having a binding relationship with the network device, a mapping relationship between identity information of associated users of the preset group and unique device identifiers that is pre-recorded in the server, and a respective network access permission corresponding to each piece of identity information; and

 a returning unit that causes the server to return the authentication result to the network device, to instruct the network device to control a network access operation of the user device according to the authentication result.

10. The apparatus of claim 9, further comprising:

a message receiving unit that causes the server to receive a notification message sent by an electronic device, the notification message including identity information that is logged in a user client of the instant messaging application running on the electronic device, and a unique device identifier of the electronic device; and

a recording unit that causes the server to record the identity information and the unique device identifier included in the notification message as a corresponding mapping relationship.

11. The apparatus of claim 9, further comprising:

a selection unit that causes the server to select a most recently recorded mapping relationship for determining the authentication result corresponding to the unique device identifier of the user device when multiple mapping relationships corresponding to the unique device identifier of the user device exist.

12. The apparatus of claim 9, wherein the associated users comprise at least one of the following: an internal member of the preset group, an external contact of the preset group, and an external visitor of the preset group.

13. A network authentication apparatus comprising:

an acquisition unit that causes a network device client running on a network device that is bound to a preset group to obtain a unique device identifier of a user device in response to the network device detecting an access of the user device;

a sending unit that causes the network device client to send an authentication request including the unique device identifier of the user device to a server of a preset instant messaging application, wherein the authentication request is used for instructing the server to perform authentication on the unique device identifier of the user device preset based on a pre-stored mapping relationship between identity information of associated users of the preset group and unique device identifiers, and a respective network access permission corresponding to each piece of identity information; and

a control unit that causes the network device client to receive an authentication result of the unique device identifier of the user device returned by the server, and control a network access operation of the user device according to the authentication result.

14. The apparatus of claim 13, wherein the control unit is specifically configured to:

cause the network device client to control the network access operation according to a value of a permission option included in the authentication result, wherein the permission option includes at least one of the following: whether the permission exists, a valid period of the permission, and a number of remaining usages of the permission, and a network range allowed to access.

15. A network authentication apparatus comprising:

a determination unit that causes a user client of a preset instant messaging application running on an electronic device to determine identity information of a logged-in user; and

a sending unit that causes the user client to send a notification message to a server of

the instant messaging application, wherein the notification message includes the identity information and a unique device identifier of the electronic device, to cause the server to record a mapping relationship between the identity information and the electronic device, wherein the mapping relationship is used for instructing the server to apply a network access permission of the identity information in a preset group to the electronic device to control the electronic device to implement a network access operation based on network device(s) under the preset group.

16. The apparatus of claim 15, wherein the sending unit causes the user client to send the notification message to the server of the instant messaging application using at least one of the following ways:

- sending the notification message when the user client detects a user login activity; and
- sending the notification message when the user client detects an access instruction for any network device.