

VERIFICATION METHOD AND APPARATUS

Technical Field

The present application relates to the field of communication technologies, and in particular, to a verification method and apparatus.

Background Art

With extensive development of the Internet technology, information security problems are particularly acute. Identity verification is generally needed when people use terminals for entertainment and shopping.

Verification methods at present generally include: password verification and environment verification. For example, when a user logs in or makes a payment, it is verified whether a password input by the user is a preset password, or whether a browser or APP (Application) used by the user has Trojans and viruses installed therein. However, this method starts verification only when an account of a user has a login or payment behavior. If a terminal of a user is lost or information of an account of the user is stolen, the security of the account of the user cannot be guaranteed.

Summary

Accordingly, the present application provides a verification method and apparatus, which may enhance the security of an account of a user.

Specifically, the present application is implemented through the following technical solutions:

A verification method, including:

receiving an operation request initiated by a user and physiologic information, of the user, collected by a device;

determining, according to the physiologic information, whether the user is in a non-operation state; and

when the user is in a non-operation state, processing, according to a preset rule, the operation request initiated by the user.

Further, the processing, according to a preset rule, the operation request initiated by the user includes:

adding at least one verification manner for an account of the user; or

rejecting the operation request initiated by the user.

Further, the method further includes:

receiving device information of the device;

storing an association relationship between the device information and the

account of the user;

acquiring device information of a device collecting the physiologic information, after the physiologic information, of the user, collected by the device is received;

determining, according to the association relationship, whether the device collecting the physiologic information is associated with the account of the user; and

determining, according to the physiologic information, whether the user is in a non-operation state if the device is associated with the account of the user.

Further, the method further includes:

sending an alert to an associated device preset by the user if the physiologic information is not received within a preset time.

Further, the physiologic information includes: one or more of heartbeat, body temperature, and pulse.

The non-operation state includes: sleeping or exercising.

Further, the device is a wearable device.

A verification method, including:

acquiring physiologic information, of a user, collected by a device;

sending the physiologic information to a server, for the server to determine, according to the physiologic information, whether the user is in a non-operation state, and when the user is in a non-operation state, process, according to a preset rule, an operation request initiated by the user.

Further, the method further includes:

acquiring device information of the device; and

sending the device information to the server, for the server to store an association relationship between the device information and an account of the user, and determine, according to the association relationship, whether a device is associated with the account of the user.

A verification apparatus, including:

a first receiving unit, configured to receive an operation request initiated by a user and physiologic information, of the user, collected by a device;

a state determining unit, configured to determine, according to the physiologic information, whether the user is in a non-operation state; and

a security control unit, configured to, when the user is in a non-operation state, process, according to a preset rule, the operation request initiated by the user.

Further, the security control unit is configured to specifically add at least one

verification manner for an account of the user; or

reject the operation request initiated by the user.

Further, the apparatus further includes:

a second receiving unit, configured to receive device information of the device;

a relationship storing unit, configured to store an association relationship between the device information and the account of the user;

the first receiving unit, configured to, after receiving the physiologic information, of the user, collected by the device, specifically acquire the device information of the device collecting the physiologic information; and

the state determining unit, configured to specifically determine, according to the association relationship, whether the device is associated with the account of the user, and determine, according to the physiologic information, whether the user is in a non-operation state if the device is associated with the account of the user.

Further, the apparatus further includes:

an alert sending unit, configured to send an alert to an associated device preset by the user if the physiologic information is not received within a preset time.

Further, the physiologic information includes: one or more of heartbeat, body temperature, and pulse; and

the non-operation state includes: sleeping or exercising.

Further, the device is a wearable device.

A verification apparatus, including:

a first acquiring unit, configured to acquire physiologic information, of a user, collected by a device;

a first sending unit, configured to send the physiologic information to a server, for the server to determine, according to the physiologic information, whether the user is in a non-operation state, and when the user is in a non-operation state, process, according to a preset rule, an operation request initiated by the user.

Further, the apparatus further includes:

a second acquiring unit, configured to acquire device information of the device; and

a second sending unit, configured to send the device information to the server, for the server to store an association relationship between the device information and an account of the user, and determine, according to the association relationship, whether the device is associated with the account of the user.

It can be seen from the above description that the present application may send to a server physiologic information, of a user, collected by a device bound by the user, such that the server may determine, according to the physiologic information, whether the user is currently in a non-operation state, and when the user is in a non-operation state, process, according to a preset rule, an operation request initiated by the user, thus enhancing the security of an account of the user, and providing real-time protection for the account of the user.

Brief Description of the Drawings

FIG. 1 is a schematic flow chart of a verification method according to an embodiment of the present application;

FIG. 2 is a schematic flow chart of a verification method according to another embodiment of the present application;

FIG. 3 is a schematic flow chart of a verification method according to another embodiment of the present application;

FIG. 4 is a schematic structural diagram of a server according to an embodiment of the present application;

FIG. 5 is a schematic structural diagram of a verification apparatus applied to a server according to an embodiment of the present application;

FIG. 6 is a schematic structural diagram of a client according to an embodiment of the present application; and

FIG. 7 is a schematic structural diagram of a verification apparatus applied to a client according to an embodiment of the present application.

Detailed Description

Exemplary embodiments will be described in detail herein, and examples thereof are shown in the accompanying drawings. In the following description involving the accompanying drawings, the same numerals in different accompanying drawings denote the same or similar elements, unless otherwise specified. Implementations described in the following exemplary embodiments do not represent all implementations consistent with the present application. In contrast, they are merely examples of apparatuses and methods consistent with some aspects of the present application as described in detail in the appended claims.

Terms used in the present application are merely used for describing specific embodiments, instead of limiting the present application. Singular forms "a(n)", "said", and "the" used in the present application and the appended claims are also

intended to include plural forms, unless clearly specified in the context to have other meanings. It should be further understood that the term "and/or" used herein refers to and includes any or all possible combinations of one or more associated items that are listed.

It should be understood that, although terms such as "first", "second", and "third" may be used in the present application to describe various kinds of information, these kinds of information should not be limited to the terms. These terms are merely used to distinguish information of the same type from each other. For example, without departing from the scope of the present application, the first information may also be referred to as the second information, and similarly, the second information may also be referred to as the first information. Depending on the context, the word "if" used herein may be explained as "when...", "as...", or "in response to the determination".

With respect to the above problems, the present application provides a verification solution, which can effectively enhance the security of an account of a user.

The present application provides a verification method, and the method is applied to a server and a client or device terminal capable of interacting with the server, respectively.

Referring to FIG. 1, the verification method applied to a server includes the following steps:

Step 101: An operation request initiated by a user and physiologic information, of the user, collected by a device are received.

In this embodiment, the user may bind an account of the user with the device, and the device includes a wearable device, for collecting the physiologic information of the user, and is capable of sending the physiologic information to the server.

The physiologic information may include: physiologic indexes such as heartbeat, body temperature, and pulse.

The operation request initiated by the user is an operation request of the user on the account of the user, such as login, modification information, and payment, which is not limited in the present application.

Step 102: It is determined, according to the physiologic information, whether the user is in a non-operation state.

Based on the step 101, after receiving the physiologic information, the server may determine, according to the physiologic information, whether the user is in a

non-operation state. The non-operation state may be understood as a state where the user cannot use the application software, for example, the user can barely use some application software when sleeping or exercising, and therefore, the non-operation state may include: sleeping or exercising.

Step 103: When the user is in a non-operation state, the operation request initiated by the user is processed according to a preset rule.

In this embodiment, if the server determines, according to the physiologic information, that the user is currently in a non-operation state, the server may process, according to the preset rule, the operation request initiated by the user to enhance the security of the account of the user. For example, the server may add a verification manner for the account of the user, reject the operation request initiated by the user, or the like.

Referring to FIG. 2, the verification method applied to a client or a device terminal includes the following steps:

Step 201: Physiologic information, of a user, collected by a device is acquired.

In this embodiment, the device may include: a wearable device. The physiologic information may include: physiologic indexes, such as heartbeat, body temperature, pulse, etc., of the user.

Step 202: The physiologic information is sent to a server, for the server to determine, according to the user information, whether the user is in a non-operation state, and when the user is in a non-operation state, process, according to a preset rule, an operation request initiated by the user.

Based on the step 201, the user may install a client on the device, and the client may acquire the physiologic information, of the user, collected by the device, and send the physiologic information to the server. Definitely, a preset program or chip may be configured on the device in advance, for sending the physiologic information to the server after the device collects the physiologic information of the user. Specifically, in this step, the user information may be sent to the server periodically, and the sending period may be set by a developer, for example, 2 seconds, which is not specially limited in the present application.

It can be seen from the above description that the present application may send physiologic information, of a user, collected by a device bound by the user to a server, such that the server may determine, according to the physiologic information, whether the user is in a non-operation state, and when the user is in a non-operation state,

process, according to a preset rule, an operation request initiated by the user, thus enhancing the security of an account of the user, and providing real-time protection for the account of the user.

A specific implementation of the present application is described below in detail with reference to embodiments.

Referring to FIG. 3, a schematic flow chart of a verification method according to an embodiment of the present application is shown, and the method includes the following steps:

Step 301: Device information of a device is acquired, and the device information is sent to a server.

In this embodiment, a user may choose, according to his/her own requirements, whether to enable the device to participate in a security decision of an account of the user, and if the user chooses to enable the device to participate in the security decision of the account of the user, the user needs to bind the device with the account of the user.

Specifically, a preset program or chip may be configured on the device, for sending the device information to the server after the device is started. Also, a client may be installed on the device, and the client may acquire device information of the device, such as a device model, and a device MAC address, and then send the device information to the server. Further, the device may be bound through a client or browser loaded on another terminal. For example, the user may log in to the account of the user through a browser, and then manually input device information of the device that the user intends to bind. Illustrations are made by taking loading a client on the device as an example in the following.

In this embodiment, the device may include: a wearable device such as a smart band and a smart watch, which is not limited in the present application.

Step 302: The server receives the device information, and stores an association relationship between the device information and the account of the user.

Based on the step 301, after receiving the device information of the device, the server may bind the device with the account of the user by storing the association relationship between the device information and the account of the user.

The user may bind the same account of the user with multiple devices. For example, the user may bind the smart band and the smart watch with a user account A used by him/her, and the server stores association relationships between the user

account A and the smart band as well as the smart watch. It should be noted that, although the user may bind multiple devices with the same account of the user, generally, the user can only select one device to participate in the security decision of the account of the user. For example, if the user first binds the smart band with the account A of the user, and then binds the smart watch with the account A of the user, a user prompt may be generated when the user performs binding, to prompt the user to select one of the smart band and the smart watch to participate in the security decision of the account of the user, and the server may store the user's selection, and set the state of the device selected by the user as an available state.

Step 303: Physiologic information, of the user, collected by the device is acquired, and the physiologic information is sent to the server.

In this embodiment, the client acquires the physiologic information, of the user, collected by the device, and the physiologic information may include: physiologic indexes, such as heartbeat, body temperature, and pulse, etc., of the user. Then, the physiologic information is sent to the server.

Specifically, in this step, the client may send the physiologic information to the server through a wireless network which the device accesses. If the device does not access a wireless network currently, the client may send the physiologic information to the server through a terminal that matches the device, which is not limited in the present application.

Step 304: The server receives an operation request initiated by the user and the physiologic information, and acquires device information of the device collecting the physiologic information.

Based on the step 303, after receiving the physiologic information sent by the client, the server acquires the device information of the device collecting the physiologic information. Specifically, when sending the physiologic information to the server, the client sends the device information of the device together to the server.

In this step, the server further receives the operation request initiated by the user on the account of the user, and the operation request includes: login, modification information, payment, and the like, which is not limited in the present application.

Step 305: The server determines, according to the association relationship, whether the device collecting the physiologic information is associated with the account of the user, and step 306 is performed if the device is associated with the account of the user. If the device is not associated with the account of the user, the

procedure is ended.

In this embodiment, the server determines, according to the device information of the device bound with the account of the user stored in step 302, whether the device collecting the physiologic information is associated with the account of the user, and if the device collecting the physiologic information is associated with the account of the user, it indicates that the device collecting the physiologic information is legal, the physiologic information is available, and step 306 is performed. If the device collecting the physiologic information is not associated with the account of the user, it indicates that the device collecting the physiologic information is not legal, the physiologic information is unavailable, and the procedure is ended.

Further, if the user binds multiple devices with the same account of the user, after the server acquires the device information of the device collecting the physiologic information, if it is determined that the device is associated with the account of the user, it is determined whether the state of the device is an available state, and if the state of the device is an available state, the physiologic information is available, and step 306 is performed. If the state of the device is an unavailable state, the physiologic information is unavailable, and the procedure is ended. For example, the user binds the smart band and the smart watch with the account A of the user, assuming that the device used by the user currently is the smart band, and the bound smart watch is used by a family member, the state of the smart band may be set as an available state, and after the server receives the physiologic information, if the physiologic information is collected by the smart band, the physiologic information is available. If the physiologic information is collected by the smart watch, the physiologic information is unavailable.

Step 306: The server determines, according to the physiologic information, whether the user is in a non-operation state, and if the user is in a non-operation state, step 307 is performed. If the user is in an operation state, the procedure is ended.

Based on the step 305, after determining that the physiologic information is available, the server determines a current state of the user according to the physiologic information. Specifically, according to physiologic indexes, such as heartbeat, body temperature, and pulse, of the user, it may be determined whether the user is currently in a non-operation state, for example, sleeping or exercising. If the user is in a non-operation state currently, step 307 is performed. If the user is in an operation state, for example, the user is not sleeping nor exercising currently, the procedure is

ended.

Step 307: The server processes, according to a preset rule, the operation request initiated by the user.

Based on the determination result of the step 306, if the user is in a non-operation state, the probability that the user uses an account of the user to make a login or payment behavior is extremely small. At this point, if the server receives the operation request initiated by the user, the probability that the operation request is initiated by the owner of the account of the user is extremely small, and the operation request may be processed according to the preset rule, to enhance the security of the account of the user. For example, at least one verification manner is added for an account of the user. The verification manner includes: one or more of two-dimensional code verification, short message verification code verification, and security question verification. Assuming that the original login verification manner of the account of the user is password verification, if the user is in the non-operation state, when receiving a login operation request for the account of the user, the server may add a short message verification code verification for the account of the user. In an extreme case, the operation request initiated by the user may be rejected when the user is in the non-operation state. Preferably, the operation request initiated by the user is rejected when multiple verifications fail. This is because, although the user is in the non-operation state, the user may lend his/her own account to another person for use, and in this step, the received operation request may be processed according to the user's pre-setting.

Optionally, in another implementation of the present application, if the server does not receive the physiologic information within a preset time, the server may send an alert to a management device preset by the user. The preset time may be set by a developer. Assuming that the client sends the user information to the server every 2 seconds, the preset time may be set as 10 seconds, that is, if the server does not receive the physiologic information within 10 seconds, the server may send an alert to a mobile phone used by the user through a mobile phone number reserved by the user.

Specifically, the server does not receive the physiologic information within the preset time, and this may be caused by a network failure or loss of the device bound by the user; at this point, the server sending an alert may remind the user to check the current situation. Further, the user may preset a processing strategy for the case that the server does not receive the physiologic information within the preset time, and the

processing strategy may include: closing login and payment functions of the account of the user, that is, rejecting all operation requests initiated by the user, or the device does not participate in the security decision of the account of the user, or the like, which is not specially limited in the present application.

It can be seen from the above description that, the present application may send the physiologic information, of the user, collected by the device bound by the user to the server, such that the server determines, according to the physiologic information, whether the user is currently in a non-operation state, and when the user is in a non-operation state, processes, according to a preset rule, the operation request initiated by the user, thus enhancing the security of the account of the user, and providing real-time protection for the account of the user.

Corresponding to the embodiment of the verification method of the present application, the present application further provides a verification apparatus. The apparatus of the present application may be implemented through software, and may also be implemented by hardware or a combination of software and hardware. By using software implementation as an example, as an apparatus in a logic sense, the verification apparatus of the present application is formed by reading a corresponding computer program instruction in a non-volatile memory, by a processor of a device thereof, into a memory for running.

Referring to FIG. 4 and FIG. 5, the present application provides a verification apparatus 400, and the verification apparatus 400 is applied to a server, including: a first receiving unit 401, a state determining unit 402, a security control unit 403, a second receiving unit 404, a relationship storing unit 405, and an alert sending unit 406.

The first receiving unit 401 is configured to receive an operation request initiated by a user and physiologic information, of the user, collected by a device.

The state determining unit 402 is configured to determine, according to the physiologic information, whether the user is in a non-operation state.

The security control unit 403 is configured to, when the user is in a non-operation state, process, according to a preset rule, the operation request initiated by the user.

Further, the security control unit 403 is configured to specifically add at least one verification manner for an account of the user; or rejects the operation request initiated by the user.

The second receiving unit 404 is configured to receive device information of the device.

The relationship storing unit 405 is configured to store an association relationship between the device information and the account of the user.

The first receiving unit 401 is configured to specifically acquire the device information of the device collecting the physiologic information, after receiving the physiologic information, of the user, collected by the device.

The state determining unit 402 is configured to specifically determine, according to the association relationship, whether the device is associated with the account of the user, and determine, according to the physiologic information, whether the user is in a non-operation state if the device is associated with the account of the user.

The alert sending unit 406 is configured to send an alert to an associated device preset by the user if the physiologic information is not received within a preset time.

Further, the physiologic information includes: one or more of heartbeat, body temperature, and pulse; and the non-operation state includes: sleeping or exercising.

Further, the device is a wearable device.

Referring to FIG. 6 and FIG. 7, the present application provides a verification apparatus 600, and the verification apparatus 600 is applied to a client, including: a first acquiring unit 601, a first sending unit 602, a second acquiring unit 603, and a second sending unit 604.

The first acquiring unit 601 is configured to acquire physiologic information, of a user, collected by a device.

The first sending unit 602 is configured to send the physiologic information to a server, for the server to determine, according to the physiologic information, whether the user is in a non-operation state, and when the user is in a non-operation state, process, according to a preset rule, an operation request initiated by the user.

The second acquiring unit 603 is configured to acquire device information of the device.

The second sending unit 604 is configured to send the device information to the server, for the server to store an association relationship between the device information and an account of the user, and determine, according to the association relationship, whether the device is associated with the account of the user.

Reference can be specifically made to the implementation processes of corresponding steps in the above method for implementation processes of functions

and effects of the units in the above apparatus, which are not repeated herein.

The above descriptions are merely preferred embodiments of the present application, and are not intended to limit the present application. Any modification, equivalent replacement and improvement made without departing from the spirit and principle of the present application shall fall within the protection scope of the present application.

Claims

1. A verification method, comprising:
 - receiving, by a receiving unit of a server, an operation request with respect to an account of a user and collected physiologic information of the user, from a client device used by the user;
 - determining, by a determining unit of the server, according to the physiologic information, whether the user is in a non-operation state to determine whether the operation request is intended by the user; and
 - when the user is determined to be in a non-operation state, processing, by a control unit of the server, according to a preset rule, the operation request with respect to the account of the user.
2. The method according to claim 1, wherein
 - the processing, according to the preset rule, the operation request with respect to the account of the user comprises:
 - adding at least one verification manner for the account of the user; or
 - rejecting the operation request with respect to the account of the user.
3. The method according to claim 1, wherein the method further comprises:
 - receiving, by the server, device information of the client device;
 - storing, by the server, an association relationship between the device information and the account of the user;
 - acquiring, by the server, device information of a client device collecting the physiologic information, after the physiologic information, of the user, collected by the client device is received;
 - determining, by the server, according to the association relationship, whether the client device collecting the physiologic information is associated with the account of the user; and
 - determining, by the server, according to the physiologic information, whether the user is in a non-operation state if the client device is associated with the account of the user.
4. The method according to claim 1, wherein the method further comprises:
 - sending an alert to an associated device preset by the user if the physiologic information is not received within a preset time.

5. The method according to claim 1, wherein
the physiologic information comprises: one or more of heartbeat, body temperature, and pulse; and
the non-operation state comprises: sleeping or exercising.
6. The method according to claim 1, wherein
the client device is a wearable device.
7. A verification method, comprising:
sending, by a sending unit of a client device used by a user, an operation request with respect to an account of a user to a server;
acquiring, by an acquiring unit of the client device, physiologic information of the user, collected;
sending the physiologic information from a sending unit of the client device to the server;
determining, by a determining unit of the server, according to the physiologic information, whether the user is in a non-operation state, to determine whether the operation request is intended by the user; and
when the user is determined to be in the non-operation state, processing, by a control unit of the server, according to a preset rule, the operation request with respect to the account of the user.
8. The method according to claim 7, wherein the method further comprises:
acquiring device information of the client device;
sending the device information from the client device to the server;
storing, by the server, an association relationship between the device information and the account of the user, and determining, by the server, according to the association relationship, whether the client device is associated of the user.
9. A verification apparatus, comprising:
a first receiving unit, configured to receive an operation request with respect to an account of a user and collected physiologic information of the user, from a client device used by the user;
a state determining unit, configured to determine, according to the physiologic information, whether the user is in a non-operation state, to determine whether the operation request is intended by the user; and
a security control unit, configured to, when the user is determined to be in a non-

operation state, process, according to a preset rule, the operation request with respect to the account of the user.

10. The apparatus according to claim 9, wherein
the security control unit is configured to add at least one verification manner for the account of the user or reject the operation request with respect to the account of the user, when the user is determined to be in the non-operation state.
11. The apparatus according to claim 9, wherein the apparatus further comprises:
a second receiving unit, configured to receive device information of the client device;
a relationship storing unit, configured to store an association relationship between the device information and the account of the user;
the first receiving unit, after receiving the collected physiologic information of the user, configured to acquire the device information of the client device collecting the physiologic information; and
the state determining unit, configured to determine, according to the association relationship, whether the client device is associated with the account of the user, and determine, according to the physiologic information, whether the user is in a non-operation state if the client device is associated with the account of the user.
12. The apparatus according to claim 9, wherein the apparatus further comprises:
an alert sending unit, configured to send an alert to an associated device preset by the user if the physiologic information is not received within a preset time.
13. The apparatus according to claim 9, wherein
the physiologic information comprises: one or more of heartbeat, body temperature, and pulse; and
the non-operation state comprises: sleeping or exercising.
14. The apparatus according to claim 9, wherein
the client device is a wearable device.