

METHOD AND APPARATUS FOR UNLOCKING USER INTERFACE

Technical Field

The present application relates to the field of terminal technologies, and in particular, to methods and apparatuses for unlocking a user interface.

Background

Due to considerations of personal privacy and data security, an increasing number of applications have a locking function added thereto, such that a corresponding user interface can be unlocked only when a correct unlocking password is inputted. However, in many situations, a user has to complete an unlocking operation while being watched by other persons, leading to the unlocking password being easily obtained by the other persons, and thus creating a severe potential security problem.

CN 103 761 038 (A) discloses a method and a device for unlocking equipment. The method comprises: when a user unlocking interface is activated, randomly selecting a feature value from a feature value set by using the equipment, and transmitting prompt information corresponding to the feature value; detecting the unlocking password input operation of a first object on a screen of the equipment; judging whether the content of the unlocking password input operation of the first object is accordant with a preset first content or not and whether the input way of the unlocking password input operation corresponds to the selected feature value, and if so, releasing the locking state of the screen of the equipment.

US 2014/059672 (A1) discloses method for generating a changing authentication input or password for a user for accessing a computing device such as a smartphone or computer.

US 2010/100948 (A1) discloses a rules driven multiple passwords system wherein a list of stored passwords are used in rotation over time in accordance with a set of rules or conditions managed by the system. The User is notified as to the newly assigned password.

Using objects displayed in sequential position on a graphic display, and input strings of text or alphanumeric characters the user has related to each object, a password can be generated by placing the input strings in an order the same as the sequence. The password can be varied easily for each access attempt by changing the objects displayed and/or the sequence.

Summary

Accordingly, the present application provides a new technical solution, which can solve a technical issue that an unlocking password is peeped at to cause a potential security problem in existing technologies.

The features of the method, apparatus and computer media according to the present invention are defined in the independent claims, and the preferable features according to the present invention are defined in the dependent claims.

To achieve the above objective, the present application provides technical solutions as follows.

According to a first aspect of the present application, a user interface unlocking method according to Claim 1 is provided.

According to a second aspect of the present application, a user interface unlocking apparatus according to Claim 7 is provided.

According to a third aspect of the present application, one or more computer-readable media according to Claim 13 are provided.

As can be seen from the above technical solutions, the present application configures a plurality of sets of unlocking passwords that are valid in a rotating manner. Even though a set of password is peeped at, an actually valid unlocking password may be selected. As such, the password that is peeped at cannot be used for releasing a locked state of a user interface, thereby facilitating a security improvement.

Brief Description of the Drawings

FIG. 1 is a flowchart of a user interface unlocking method according to an exemplary embodiment of the present application.

FIG. 2 is a flowchart of a user interface unlocking method according to another exemplary embodiment of the present application.

FIG. 3 – FIG. 7 are schematic diagrams of an interface according to exemplary embodiments of the present application.

FIG. 8 is a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application.

FIG. 9 is a block diagram of a user interface unlocking apparatus according to an exemplary embodiment of the present application.

Detailed Description

The following embodiments are provided for description of the present application in further detail.

Referring to FIG. 1, FIG. 1 shows a user interface unlocking method according to an exemplary embodiment of the present application, which may be applicable in a terminal. The method includes the following steps.

Step 102 selects, when an unlocking interface is triggered, an unlocking password applicable to the current unlocking interface from a plurality of preset sets of passwords.

In the present embodiment, a user may set up multiple sets of passwords corresponding to each unlocking interface in advance. The number of passwords may be set according to needs, for example, 3 sets or 5 sets. A specific number thereof is not limited in the present application. Each unlocking interface has a corresponding application, and the unlocking interface is used for restricting privileges of a user to access data or information in the application, for example, a desktop loading program (corresponding to a lock screen interface of a mobile phone) or any APP (Application) such as "AlipayTM" installed in a terminal.

In the present embodiment, different unlocking interfaces may separately be provided with corresponding sets of passwords. Alternatively, the same sets of passwords may be shared by multiple unlocking interfaces.

In the present embodiment, each time a user triggers an unlocking interface, a current valid password (i.e., an unlocking password) is re-selected, thus facilitating an improvement

in security as compared with a manner of adopting a single password only in existing technologies.

Step 104 unlocks a locked state of the interface in response to receiving a user input password that matches the unlocking password.

As can be seen from the above embodiment, the present application sets multiple sets of passwords for an unlocking interface and selects a valid password from the multiple sets of passwords when the unlocking interface is triggered, such that the same unlocking interface may be corresponding to different unlocking passwords in multiple unlocking processes. As such, even though an unlocking password inputted by a user has been peeped at by another person, the same password is most likely unable to unlock the corresponding unlocking interface, thereby significantly improving the security.

The technical solution of the present application is described in detail with reference to specific application scenarios hereinafter. Referring to FIG. 2, FIG. 2 shows a user interface unlocking method according to an exemplary embodiment of the present application, which includes the following steps:

Step 202 configures multiple sets of passwords according to a user operation.

In the present embodiment, multiple sets of passwords are assumed to be set up by a user for a terminal lock screen interface. The multiple sets of passwords that are set may only be used for the terminal lock screen interface, and may also be applicable to another lock screen interface. The user may perform configuration according to needs.

When setting up passwords for a lock screen interface of a terminal, a user may first switch to a "Password Lock" interface as shown in FIG. 3, to configure password-related options. As shown in FIG. 3, the terminal may have three sets of passwords set up by default, namely, a password 1, a password 2, and a password 3. Apparently, the user may select only

two sets of passwords thereof according to an actual requirement, or set up more sets of passwords by selecting "More". In a configuration interface as shown in FIG. 3, a corresponding pattern is provided before each set of password. For example, the password 1 corresponds to "○", the password 2 corresponds to "□", and the password 3 corresponds to "△", such that the sets of passwords can be effectively distinguished from each other. If the user needs to configure the password 1, the user may switch to a "Set password 1" interface as shown in FIG. 4 by sliding a "Slider" icon behind the password 1.

As shown in FIG. 4, the user may perform an input operation via a keyboard at the bottom of the interface, thereby implementing the configuration of the password 1. At the same time, "Distinguishing identifier: ○" is displayed on the interface to prompt the user to conduct an associative memory between such pattern and the password 1. Therefore, accurate input can be achieved during usage.

Step 204 triggers an unlocking interface.

In the present embodiment, a lock screen interface of a terminal is used as an example. A triggering may occur in response to detecting that "power button", "volume button", "home button" or another type of physical button on the terminal is pressed. Moreover, a triggering may occur in response to detecting that a light change, a spatial position change or another parameter meets a preset parameter, A specific embodiment includes switching a screen of the terminal from a non-display state (i.e., "black screen") to a display state. An APP in a terminal is used as an example. In response to detecting that a corresponding program icon is pressed, a corresponding unlocking interface may be triggered.

Step 206 determines a historical password that is most recently used.

In the present embodiment, if a current triggering and unlocking activity is the (N+1)th one that is performed on a lock screen interface of a terminal, a "historical password that is

most recently used" is a password used when an unlocking operation is performed on the lock screen interface of the terminal at the N^{th} time.

Set	Password	Invalid identifier
1	1362	1
2	0724	0
3	2014	0

Table 1

Specifically, an available state of each set of password may be marked to determine a "historical password that is most recently used". For example, a user sets three sets of passwords for a terminal lock screen interface: "Password 1: 1362", "Password 2: 0724", and "Password 3: 2014", as shown in Table 1. A value of an invalid identifier corresponding to the password 1 is 1, and values of invalid identifiers corresponding to the password 2 and the password 3 are 0, indicating that the password 1 is the password that is used at the N^{th} time (i.e., the "historical password that is most recently used").

Step 208 determines a current valid password.

In the present embodiment, upon determining that the "historical password applied recently" is the password 1, an unlocking password applied to a current unlocking operation, i.e., a "current valid password", may be selected from among the remaining password 2 and password 3. Therefore, the password 1 cannot be used for the current $(N+1)^{\text{th}}$ unlocking operation, even though having been recorded by another person during the N^{th} unlocking operation.

As an exemplary implementation, when a current valid password is selected, the remaining password 2 and password 3 may be selected sequentially according to a preset order of the multiple sets of passwords. For example, if the order of the multiple sets of passwords is an order of arrangement of entries in Table 1: password 1→password 2→

password 3→password 1, the password 2 is to be selected accordingly as the current valid password when the password 1 is an invalid password. Similarly, if the password 2 is an invalid password, the password 3 is to be selected in turn as the current valid password. If the password 3 is an invalid password, the password 1 is to be selected in turn as the current valid password. If the order of the multiple sets of passwords is another order: password 1→password 3→password 2→password 1... ..., the password 3 is to be selected in turn as the current valid password when the password 1 is an invalid password. Similarly, if the password 2 is an invalid password, the password 1 is to be selected in turn as the current valid password, and if the password 3 is an invalid password, the password 2 is to be selected in turn as the current valid password.

As another exemplary implementation, according to storage positions of entries corresponding to the multiple sets of passwords in Table 1, a password adjacent to an invalid password may also be selected as a current valid password. For example, when the password 1 is an invalid password, the password 2 adjacent thereto may be selected as a valid password.

As another exemplary implementation, a set of password may be randomly selected as a current valid password from among all remaining passwords other than an invalid password.

Apparently, as another exemplary embodiment, step 206 and step 208 may not be used to select a current valid password, and the current valid password may be randomly selected directly from the corresponding multiple sets of passwords each time when the terminal lock screen interface is triggered, to ensure the security through the randomness of password selection.

Step 210 performs a corresponding prompt operation according to the determined

current valid password.

In the present embodiment, by performing a prompt operation, a user who has a true usage permission may know a current valid password and input a correct password. A number of approaches of performing a prompt operation exist, and any approach that is able to establish a unique correspondence between a prompt operation and a password is applicable to the technical solutions of the present application.

As an exemplary implementation, the password 1, the password 2, and the password 3 in FIG. 3 each have corresponding patterns individually. Therefore, a corresponding pattern may be displayed on a terminal lock screen interface to implement a prompt operation. For example, as shown in FIG. 5, if the current valid password is the password 1, a "password display box" may be set as "○" corresponding to the password 1, i.e., "○○○○" as shown in FIG. 5(a) (the number of "○" here corresponds to the number of digits of the password, i.e., the password in the current example has 4 digits). If the current valid password is the password 2, the "password display box" may be set as "□" corresponding to the password 2, i.e., "□□□□" as shown in FIG. 5(b). If the current valid password is the password 3, the "password display box" may be set as "△" corresponding to the password 3, i.e., "△ △ △ △" as shown in FIG. 5(c).

In fact, patterns such as "○", "□" and "△" in the examples as shown in FIG. 5 all belong to visual identifying information, i.e., identifying information for recognition and differentiation through a visual difference. Similarly, effective differentiation of different passwords may also be implemented by, for example, pictures, dynamic pictures, background colors, numerical buttons or colors of characters therein, colors of a password display box, etc.

Moreover, other forms of prompt operations may also be used to achieve distinguishing

between different passwords. For example, as another exemplary implementation, if prompt information is a multimedia file, i.e., an audio file, a video file, etc., the multimedia file may be played to mark a password from an auditory perspective or an auditory and visual perspective. Specifically, a play button as shown in FIG. 6 may be set on the terminal unlocking interface, and a corresponding multimedia file may be played by clicking the button. For another example, as another exemplary implementation, if prompt information is vibration control information, different vibration effects (such as vibration strength and vibration time, etc.) may be implemented by a control terminal to identify passwords. One skilled in the art should understand that a specific form of a prompt operation is not limited herein, and any technical measure that is able to distinguish multiple sets of passwords is applicable to the technical solutions of the present application.

Step 212 receives a password inputted by a user.

In the present embodiment, when the password is a numerical password as shown in Table 1, e.g., the password 1 "1362", the user may input a corresponding combination of numerals through a number key pad in FIG. 5(a). Apparently, the "numerical password" is merely an exemplary implementation of an unlocking password in the present application. In another exemplary implementation, the unlocking password may use a "gesture pattern" as shown in FIG. 7, for example.

For example, each node in FIG. 7(a) is "○", and the current valid password is the password 1 as shown in Table 1. Each node in FIG. 7(b) is "□", and the current valid password is the password 2 as shown in Table 1. Each node in FIG. 7(c) is "△", and the current valid password is the password 3 as shown in Table 1. Apparently, one skilled in the art should understand that a specific form of an unlocking password is not limited herein, and other forms of unlocking passwords are apparently applicable to the technical solutions of the

present application.

Step 214 determines whether the password inputted by the user matches the current valid password, proceeds to step 216 if matched, or proceeds to step 218 otherwise.

Step 216 proceeds to step 220, and unlocking is successful.

Step 218 proceeds to step 212, and the unlocking fails.

Step 220 adds an invalid identifier for the current password, and removes an invalid identifier of the historical password (i.e., the "historical password that is most recently used") determined at step 206.

In the present embodiment, after the "historical password that is most recently used" is identified by the "invalid identifier" at step 206, the terminal lock screen interface is unlocked as the password inputted by the user at step 214 matches the current valid password. Therefore, the $(N+1)^{\text{th}}$ unlocking operation performed on the terminal lock screen interface is completed, and the "historical password that is most recently used" is updated to the password used when the $(N+1)^{\text{th}}$ unlocking operation is performed on the terminal lock screen interface.

For example, if the unlocking password used at the $(N+1)^{\text{th}}$ time is the password 2, a value of an invalid identifier corresponding to the password 2 needs to be modified to "1", and a value of an invalid identifier corresponding to the password 1 needs to be modified to "0", as shown in Table 2. Therefore, when triggering and unlocking operations are performed on the terminal lock screen interface for the $(N+2)^{\text{th}}$ time, the password 2 will not be selected.

Set	Password	Invalid identifier
1	1362	0
2	0724	1
3	2014	0

Table 2

In addition, it should be noted that:

The "unlocking control type in a current unlocking interface" may be understood as: multiple types of unlocking controls may be used for the same unlocking interface, such as a "keyboard input" type (as shown in FIG. 4 to FIG. 6), a "nine-grid pattern" type (as shown in FIG. 7, including $3 \times 3 = 9$ contact points), and a "sixteen-grid pattern" type (including $4 \times 4 = 16$ contact points, which is similar to the "nine-grid pattern" and is not shown in the drawing). A user may set up an individual password corresponding to each unlocking control type, such that a corresponding unlocking password may be determined based on an unlocking control type used in a current unlocking interface. Correspondingly, passwords of the same unlocking control type may be used as the "multiple sets of passwords" in the present application, for example, all of a character type that needs to be inputted (corresponding to an unlocking control of the "keyboard input" type) or a gesture type (corresponding to an unlocking control of the "nine-grid pattern" type or "sixteen-grid pattern" type).

Alternatively, passwords of multiple unlocking control types may also be used.

FIG. 8 is a schematic structural diagram of an electronic device according to an exemplary embodiment of the present application. Referring to FIG. 8, on a hardware level, the electronic device includes processor(s), an internal bus, a network interface, memory, and a non-volatile storage device, and may apparently further include hardware required by other services. The processor(s) read(s) a corresponding computer program from the non-volatile storage device into the memory and runs the computer program, thereby forming a user interface unlocking apparatus on a logic level. Apparently, besides software implementation, the present application does not exclude other implementations, such as implementations in a form of logic devices or a combination of software and hardware. In other words, executing entities in the following flow of processing may include, but not limited to, various logic units, and may also include hardware or logic devices.

Referring to FIG. 9, in a software implementation, the user interface unlocking apparatus may include a selection unit and an unlocking unit.

The selection unit is configured to select, when an unlocking interface is triggered, an unlocking password applicable to the interface from among multiple preset sets of passwords.

The unlocking unit is configured to release a locked state of the interface in response to receiving a user input password that matches the unlocking password.

Optionally, the selection unit is specifically configured to determine a historical password that is most recently applied to the current unlocking interface, and select the unlocking password from remaining passwords in the multiple sets of passwords.

Optionally, the selection unit is specifically configured to select a set of password provided with an invalid identifier as the historical password from the multiple sets of

passwords.

The apparatus further includes an identifier processing unit configured to add the invalid identifier for the unlocking password when the user input password matching the unlocking password is received, and remove the invalid identifier corresponding to the historical password.

Optionally, the selection unit is specifically configured to use a set of password that is adjacent to the historical password as the unlocking password based on the historical password and a preset order of the multiple sets of passwords.

Optionally, the apparatus further includes a prompt unit configured to determine prompt information corresponding to the unlocking password, and perform a prompt operation according to the prompt information.

Optionally, the prompt information includes at least one of the following: visual identifying information, a multimedia file, and vibration control information.

By setting up multiple sets of unlocking passwords that are valid successively, the present application can therefore select an actually valid unlocking password even though a certain set of password has been peeped at. As such, the password that has been peeped at cannot be used for unlocking a locked state of a user interface, thereby facilitating an improvement in the security.

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

The memory may include a form of computer-readable media, e.g., a non-permanent storage device, random-access memory (RAM) and/or a nonvolatile internal storage, such as read-only memory (ROM) or flash RAM. The memory is an example of computer-readable media.

The computer-readable media may include a permanent or non-permanent 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 should be further noted that terms such as "comprise", "include" and any other variants thereof are intended to cover a non-exclusive inclusion. A process, method, product or device that includes a series of elements not only includes those elements, but also includes other elements that are not explicitly listed, or further includes elements that already existed in such process, method, product or device. In a condition without further limitations, an element defined by a phrase "include a/an ..." does not exclude any other similar elements from existing in the process, method, product or device.

The above descriptions are merely preferred embodiments of the present application, and are not intended to limit the present application. Any modifications, equivalent replacements and improvements made without departing from the spirit and principles of the present application shall fall within the scope of protection of the present application.

Claims

1. A user interface unlocking method, carried out by a user interface unlocking apparatus, comprising:

in response to an unlocking interface being triggered:

selecting (208), an unlocking password applicable to the interface from a plurality of preset, stored passwords, the selecting (208) the unlocking password comprising:

determining (206) a historical password that is most recently applied to the unlocking interface, the determining (206) comprising selecting a password provided with an invalid identifier as the historical password from the plurality of preset, stored passwords, wherein the invalid identifier was previously added (220) to a previous unlocking password in response to receiving a user input password that matched (214) the previous unlocking password, so identifying that previous unlocking password as the historical password, and a respective invalid identifier corresponding to a previous historical password was removed; and

selecting (208) the unlocking password from remaining passwords other than the historical password in the plurality of preset, stored passwords;

and performing (210) a prompt operation corresponding to the selected unlocking password;

In response to receiving a user input password that does not match (218) the unlocking password, prompting the user to input password again (210);

or in response to receiving a user input password that matches (214) the unlocking password, releasing (216) a locked state of the interface, removing the invalid identifier from the historical password and adding the invalid identifier to the unlocking password.

2. The method of claim 1, wherein selecting (208) the unlocking password from the remaining passwords in the plurality of preset, stored passwords comprises using a password that is adjacent to the historical password as the unlocking password based on the historical password and a preset order of the plurality of passwords.

3. The method of claim 1 or claim 2, further comprising:
determining prompt information corresponding to the unlocking password; and
performing (210) a prompt operation according to the prompt information.

4. The method of claim 3, wherein the prompt information comprises at least one of the following: visual identifying information, a multimedia file, or vibration control information.

5. A user interface unlocking apparatus comprising:
a selection unit configured to select (208), in response to an unlocking interface being triggered, an unlocking password applicable to the interface from a plurality of preset, stored passwords, the selection unit being configured to determine (206) a historical password that is most recently applied to the unlocking interface, and select (208) the unlocking password from remaining passwords other than the historical password in the plurality of preset, stored passwords, and additionally to select a password provided with an invalid identifier as the historical password from among the plurality of preset, stored passwords, wherein the invalid identifier was previously added (220) to a previous unlocking password in response to receiving a user input password that matched (214) the previous

unlocking password, so identifying that previous unlocking password as the historical password, and a respective invalid identifier corresponding to a previous historical password was removed;

an identifier processing unit configured to add (220) the invalid identifier for the unlocking password when the user input password matching (214) the unlocking password is received, and remove a respective invalid identifier corresponding to the historical password;

a prompt unit configured to perform (210), in response to the unlocking interface being triggered, a prompt operation corresponding to the selected unlocking password;

and

an unlocking unit configured to, in response to receiving a user input password that does not match (218) the unlocking password, prompt the user to input password again (210); or in response to receiving a user input password that matches (214) the unlocking password, release (216) a locked state of the interface when a user input password matching the unlocking password is received, and wherein the identifier processing unit is configured to, in response to receiving the user input password that matches (214) the unlocking password, remove the invalid identifier from the historical password and add the invalid identifier to the unlocking password.

6. The apparatus of claim 5, wherein the selection unit is configured to use a password that is adjacent to the historical password as the unlocking password based on the historical password and a preset order of the plurality of preset, stored passwords.

7. The apparatus of claim 5 or claim 6, further comprising a prompt unit configured to determine prompt information corresponding to the unlocking password, and perform (210) the prompt operation according to the prompt information.

8. The apparatus of claim 7, wherein the prompt information comprises at least one of the following: visual identifying information, a multimedia file, or vibration control information.

9. One or more computer-readable media storing executable instructions that, when executed by one or more processors, cause the one or more processors to perform acts comprising:

in response to the unlocking interface being triggered, selecting (208) an unlocking password applicable to an unlocking interface from a plurality of preset, stored passwords, the selecting (208) the unlocking password comprising:

determining (206) a historical password that is most recently applied to the unlocking interface, the determining (206) comprising selecting a password provided with an invalid identifier as the historical password from the plurality of preset, stored passwords, wherein the invalid identifier was previously added (220) to a previous unlocking password in response to receiving a user input password that matched (214) the previous unlocking password, so identifying that previous unlocking password as the historical password, and a respective invalid identifier corresponding to a previous historical password is removed; and

selecting (208) the unlocking password from remaining passwords of the plurality of preset, stored passwords;

and performing (210) a prompt operation corresponding to the selected unlocking password;

in response to receiving a user input password that does not match (218) the unlocking password, prompting the user to input password again (210);

or in response to receiving a user input password that matches (214) the unlocking password, releasing (216) a locked state of the unlocking interface, removing the invalid identifier from the historical password and adding the invalid identifier to the unlocking password.