

LEAKAGE RESILIENT PASSWORD SYSTEM AND METHOD

FIELD OF THE INVENTION

[0001] The invention pertains to the field of reducing the probability of passwords being leaked.

BACKGROUND

[0002] Mobile devices are ubiquitous for connecting users to the cyberspace. A user may use a smartphone, tablet, or wearable device to access not only general informative services but also sensitive services such as mobile banking and corporate services. In order to prevent unauthorized access to these services, user authentication is required to verify the identity of a user. Password-based authentication is still the most pervasive due to significant advantage in usability over other alternatives such as smartcards and biometrics.

[0003] However, password-based user authentication suffers from an intrinsic weakness of password leakage during password entry, which may reveal passwords to surrounding attackers (e.g., by shoulder surfing and key logging). This threat is compounded in scenarios when mobile devices are involved, as mobile devices are widely used in public places.

[0004] It is therefore an object of an invention to solve the above deficiencies and at least provide a novel leakage resilient password system and method.

SUMMARY OF INVENTION

[0005] The invention will now be described in detail with reference to the accompanying drawings.

[0006] According to a first aspect of the invention, a system for accepting entry of a password is described, the password comprising at least one password character, the system comprising a display unit; a secure means for implementing a secure channel for the display unit such that the display unit is visible only to a user providing a user entry, the secure

1 channel being removed upon deactivation of the secure means; a processing unit configured to
2 generate a plurality of randomly arranged shadow-pad buttons interposed with a plurality of
3 keypad buttons, each one of the plurality of keypad buttons bearing a keypad character, and
4 each one of the plurality of shadow-pad buttons bearing a shadow-pad character, and each one
5 of the plurality of shadow-pad buttons being associated with one of the plurality of keypad
6 buttons. The system further describes a memory unit for storing the plurality of shadow-pad
7 buttons interposed with the plurality of keypad buttons; and an input unit for accepting the
8 user entry upon the removal of the secure channel. Wherein the processing unit is further
9 configured to display on the display unit the plurality of shadow-pad buttons interposed with
10 the plurality of keypad buttons upon the implementation of the secure channel, each one of the
11 plurality of shadow-pad buttons having a visual effect to indicate the association with one of
12 the plurality of keypad buttons. Wherein the at least one password character matches the
13 keypad character of one of the plurality of keypad buttons, the shadow-pad character of the
14 shadow-pad button associated with the matched keypad button indicates that the shadow-pad
15 character should be selected as the user entry upon the removal of the secure channel; and
16 wherein the processing unit is further configured to recognize that the at least one password
17 character has been entered when the shadow-pad character is entered as the user entry.

18
19 [0007] Preferably, the system further comprises an output unit and the processing unit
20 is further configured to send the at least one password character to the output unit for
21 authentication.

22
23 [0008] Preferably, the secure means is a hand-shielding gesture over a gesture
24 detection area.

25
26 [0009] Preferably, at least one of the plurality of keypad buttons has a plurality of
27 associated shadow-pad buttons.

28
29 [0010] Preferably, the display unit, processing unit, memory unit and input unit are
30 part of a portable handheld device or an automated teller machine or a computer terminal.

31
32 [0011] Preferably, the shadow pad character is selected either by touching a keypad button or
33 by voice input received by the input unit.

34
35 [0012] According to a second aspect of the invention, a method for accepting entry of
36 a password is described, the password comprising at least one password character, the method

1 comprising the steps of generating with a processing unit, a plurality of randomly arranged
2 shadow-pad buttons interposed with a plurality of keypad buttons, each one of the plurality of
3 keypad buttons bearing a keypad character, and each one of the plurality of shadow-pad
4 buttons bearing a shadow-pad character, and each one of the plurality of shadow-pad buttons
5 being associated with one of the plurality of keypad buttons; and storing the plurality of
6 shadow-pad buttons interposed with the plurality of keypad buttons into a memory unit. The
7 method further comprises the steps of implementing with a secure means a secure channel for
8 a display unit such that the display unit is visible only to a user providing a user entry; and
9 displaying on the display unit, the plurality of shadow-pad buttons interposed with the
10 plurality of keypad buttons, each one of the plurality of shadow-pad buttons having a visual
11 effect to indicate the association with one of the plurality of keypad buttons; wherein the at
12 least one password character matches the keypad character of one of the plurality of keypad
13 buttons. The method further comprises the steps of removing the secure channel by
14 deactivating the secure means; accepting the user entry with an input unit, the user entry
15 being the shadow-pad character of the shadow-pad button associated with the matched keypad
16 button; and recognizing with the processing unit, that the at least one password character has
17 been entered.

18
19 [0013] Preferably, the method further comprises the step of sending with the
20 processing unit, the at least one password character to an output unit for authentication.

21
22 [0014] Preferably, the method further comprises the step of implementing a secure
23 channel with a secure means comprises the step of placing a hand-shielding gesture over a
24 gesture detection area.

25
26 [0015] According to a third aspect of the invention, a wearable device for accepting
27 entry of a password when worn on a user's head is described, the password comprising at least
28 one password character, the wearable device comprising an optical head mounted display; a
29 processing unit configured to generate a plurality of randomly arranged shadow-pad buttons
30 interposed with a plurality of keypad buttons, each one of the plurality of keypad buttons
31 bearing a keypad character, and each one of the plurality of shadow-pad buttons bearing a
32 shadow-pad character, and each one of the plurality of shadow-pad buttons being associated
33 with one of the plurality of keypad buttons; a memory unit for storing the plurality of shadow-
34 pad buttons interposed with the plurality of keypad buttons; and a voice recognition device for
35 processing a voice input. Wherein the processing unit is further configured to display on the

1 optical head mounted display the plurality of shadow-pad buttons interposed with the plurality
2 of keypad buttons, each one of the plurality of shadow-pad buttons having a visual effect to
3 indicate the association with one of the plurality of keypad buttons. Wherein the at least one
4 password character matches the keypad character of one of the plurality of keypad buttons, the
5 shadow-pad character of the shadow-pad button associated with the matched keypad button
6 indicates that the shadow-pad character should be selected as the voice input; and wherein the
7 processing unit is further configured to determine that the at least one password character has
8 been entered when the shadow-pad character is entered as the voice input.

9
10 [0016] Preferably, at least one of the plurality of keypad buttons has a plurality of
11 associated shadow-pad buttons.

12
13 [0017] According to a fourth aspect of the invention, a method for accepting entry of a
14 password with a wearable device when worn on a user's head is described, the password
15 comprising at least one password character, the method comprising the steps of generating
16 with a processing unit of the wearable device, a plurality of randomly arranged shadow-pad
17 buttons interposed with a plurality of keypad buttons, each one of the plurality of keypad
18 buttons bearing a keypad character, and each one of the plurality of shadow-pad buttons
19 bearing a shadow-pad character, and each one of the plurality of shadow-pad buttons being
20 associated with one of the plurality of keypad buttons; storing the plurality of shadow-pad
21 buttons interposed with the plurality of keypad buttons into a memory unit of the wearable
22 device; displaying on an optical head mounted display of the wearable device, the plurality of
23 shadow-pad buttons interposed with the plurality of keypad buttons each one of the plurality
24 of shadow-pad buttons having a visual effect to indicate the association with one of the
25 plurality of keypad buttons; wherein the at least one password character matches the keypad
26 character of one of the plurality of keypad buttons. The method further comprises the steps of
27 accepting a voice input with a voice recognition device of the wearable device, the voice input
28 being the shadow-pad character of the shadow-pad button associated with the matched keypad
29 button; and determining with the processing unit, that the at least one password character has
30 been entered.

31
32 [0018] The invention will now be described in detail with reference to the
33 accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The accompanying figures illustrate disclosed embodiment(s) and serve to explain principles of the disclosed embodiment(s). It is to be understood, however, that these drawings are presented for purposes of illustration only, and not for defining limits of the application.

[0020] Figure 1 shows a leakage resilient password system in accordance with a preferred embodiment of the invention.

[0021] Figure 2 shows an exemplary example of a secure means.

[0022] Figure 3 shows input unit displaying keypad buttons interposed with shadow-pad buttons in accordance with a preferred embodiment of the invention.

[0023] Figures 4(a), 4(b), 4(c), 4(d), 4(e) and 4(f) illustrate the permutations of input unit in accordance with the invention.

[0024] Figure 5 shows a flowchart that illustrates a method in accordance with a preferred embodiment of the invention.

[0025] Figure 6 shows an alternative embodiment of the invention where a keypad button is associated with a plurality of shadow-pad buttons.

[0026] Figure 7 shows a flowchart that illustrates a method in accordance with another preferred embodiment of the invention.

[0027] Figure 8 shows a keypad partitioned into a plurality of partitioned keypads.

[0028] Figure 9 shows a flowchart that illustrates a method in accordance with another preferred embodiment of the invention.

[0029] Exemplary, non-limiting embodiments of the present application will now be described with references to the above-mentioned figures.

DETAILED DESCRIPTION

1 [0030] Figure 1 shows a leakage resilient password system 100 in accordance with a
2 preferred embodiment of the invention. System 100 comprises display unit 101 and secure
3 means 102. System 100 further comprises input unit 103, processing unit 104, output unit 105
4 and memory 106.

5
6 [0031] Display unit 101 can be a screen of a mobile device. Secure means 102 can be
7 a hand-shielding gesture as shown in Figure 2. Secure means 102 results in a secure channel
8 such that what is being displayed on display unit 101 can be visible and discernible only to the
9 user. Input unit 103 is located in a portion of display unit 101. Input unit 103 can be touch-
10 screen keypads. Optionally, input unit can also comprise voice activation software, where the
11 display unit shows data orally communicated by the user via a voice input.

12
13 [0032] Processing unit 104 can be a microprocessor. Processing unit 104 can
14 read/write to memory 106. Processing unit 104 can generate shadow-pads 303. Processing
15 unit 104 can send information to display unit 101 to display keypad 301 and shadow-pad 303
16 (see figure 3). Processing unit 104 can accept user's input via input unit 103. Processing unit
17 104 can also output the user's password to output unit 105, which can be sent to any user
18 authentication application such as unlocking a device, activating a password manager,
19 accessing a user account, or making a payment.

20
21 [0033] Once processing unit 104 detects that secure means 102 has provided a secure
22 channel, processing unit 104 will send information to display unit 101 to display keypad 301
23 and shadow-pad 303 as shown in figure 3. Processing unit 104 can detect that secure means
24 102 (Hand A) has provided a secure channel when the hand-shielding gesture is placed over
25 gesture detection area 107 as shown in figure 2.

26
27 [0034] Figure 3 shows keypad 301 having keypad buttons 302. Figure 3 also shows
28 shadow-pad 303 having shadow-pad buttons 304. Each keypad button 302 and shadow-pad
29 button 304 bears or presents a character. A character can be any alphabetical letter, digit,
30 punctuation or symbol. Shadow-pad 303 with its shadow-pad buttons 304 are essentially a
31 randomly re-shuffled version of keypad 301 and its keypad buttons 302 such that the
32 characters presented by shadow-pad buttons 304 are non-sequential and random in nature as
33 shown in figure 3. Each shadow-pad button 304 is associated with one keypad button 302. As
34 shown in figure 3, shadow-pad buttons 304 are interposed with keypad buttons 302. Shadow-
35 pad buttons 304 are located adjacent and proximate to its associated keypad button 302 as

1 shown in figure 3. Shadow-pad button 304 has to be located proximate to its associated
2 keypad button 302, and away from the neighboring keypad button 302 to such an extent that a
3 user would not be confused as to which keypad button 302 shadow-pad button 304 is
4 associated to. Shadow-pad button 304 can also have a graphic to indicate its association with
5 keypad button 302. For example, in figure 3, shadow-pad button 304 has a "shadow-like"
6 effect graphic to indicate its association with keypad button 302.

7
8 [0035] The character as presented in shadow-pad button 304 indicate to the user the
9 keypad button 302 the user should select to input the password character or intended character
10 (the character the user intends to input). For example, referring to figure 3, shadow-pad button
11 304 bearing character "5" is associated with keypad button 302 bearing character "1". This
12 indicates to the user that to enter the intended character "1", once secure means 102 is
13 removed, the user would have to select keypad button 302 bearing the character "5". In
14 another example found in figure 3, shadow-pad button 304 bearing the character "9" is
15 associated with keypad button 302 bearing the character "2". This indicates to the user that to
16 enter the intended character "2", once secure means 102 is removed, the user would have to
17 select keypad button 302 bearing the character "9". Alternatively, shadow-pad character
18 selection may be made by voice input, for those devices with input units capable of receiving
19 voice input.

20
21 [0036] Figures 4(a), 4(b), 4(c), 4(d), 4(e) and 4(f) illustrate the permutations of keypad
22 301 and shadow-pad 303 in accordance with the invention. In this illustration, the password of
23 the user has the following string of characters: "3" "7" "4".

24
25 [0037] Processing unit 104 generates an instance of shadow-pad 303 with its shadow-
26 pad buttons 304 and stores this instance of shadow-pad 303 in memory 106. Shadow-pad 303
27 with its shadow-pad buttons 304 are essentially a randomly re-shuffled version of keypad 301
28 and its keypad buttons 302 such that the characters presented by shadow-pad buttons 304 are
29 non-sequential and random in nature. Each shadow-pad button 304 of this instance of shadow-
30 pad 303 is associated with one keypad button 302 of keypad 301. This association is also
31 stored in memory 106. When secure means 102 is applied and a secure channel is detected,
32 processing unit 104 displays this instance of shadow-pad 303 with its shadow-pad buttons 304
33 and its associated keypad buttons 302 of keypad 301 on display unit 101 as shown in figure
34 4(a).

1 [0038] Shadow-pad button 304 bearing the character "7" associated with keypad
2 button 302 bearing the character "3" indicates to the user that to enter the intended character
3 "3", once secure means 102 is removed, the user would have to select keypad button 302
4 bearing the character "7".

5
6 [0039] Once secure means 102 is removed, input unit 103 displays only keypad 301
7 and its keypad buttons 302 as shown in figure 4(b). Shadow-pad 303 and its shadow-pad
8 buttons 304 are not displayed once secure means 102 is removed. The user selects keypad
9 button 302 bearing the character "7". Based on the stored instance of shadow-pad 303 with its
10 shadow-pad buttons 304 and their association with keypad buttons 302 in memory 106,
11 processing unit 104 is able to determine that "3" was the intended character. Processing unit
12 104 stores the intended character "3" in memory 106. If however the user fails to select any
13 keypad button 302 after a predetermined amount of time, or the user inputs a "cancel" at any
14 time, then processing unit 104 clears memory 106 of the instance of shadow-pad 303 with its
15 shadow-pad buttons 304 and stops the process.

16
17 [0040] Processing unit 104 generates a new instance of shadow-pad 303 with its
18 shadow-pad buttons 304, and replaces the previous instance of shadow-pad 303 with the new
19 instance of shadow-pad 303 in memory 106. The shadow-pad buttons 304 in this instance of
20 shadow-pad 303 are randomly arranged such that the arrangement of the characters presented
21 by shadow-pad buttons 304 will be different to the previous instance of shadow-pad 303.
22 Each shadow-pad button 304 of this instance of shadow-pad 303 is associated with one
23 keypad button 302 of keypad 301.

24
25 [0041] When secure means 102 is reapplied and a secure channel is detected,
26 processing unit 104 displays this new instance of shadow-pad 303 with its shadow-pad buttons
27 304 and its associated keypad buttons 302 of keypad 301 on display unit 101 as shown in
28 figure 4(c). Shadow-pad button 304 bearing the character "0" associated with keypad button
29 302 bearing the character "7" indicates to the user that to enter the intended character "7",
30 once secure means 102 is removed, the user would have to select keypad button 302 bearing
31 the character "0".

32
33 [0042] As mentioned above, shadow-pad buttons 304 are randomly arranged. This is
34 to ensure that arrangement of the characters presented by shadow-pad buttons 304 in each
35 instance of shadow-pad 303 is different. For example, the arrangement of the characters
36 presented by shadow-pad buttons 304 in the instance of shadow-pad 303 generated in figure

1 4(a) is different from the arrangement of the characters presented by shadow-pad buttons 304
2 in the instance of shadow-pad 303 generated in figure 4(c). This is to ensure that the
3 arrangement of the characters presented by shadow-pad buttons 304 in shadow-pad 303 does
4 not exhibit any discernable pattern which enhances security.

5
6 [0043] Once secure means 102 is removed, input unit 103 displays only keypad 301
7 and its keypad buttons 302 as shown in figure 4(d). Shadow-pad 303 and its shadow-pad
8 buttons 304 are not displayed once secure means 102 is removed. The user selects keypad
9 button 302 bearing the character "0". Based on the stored instance of shadow-pad 303 with its
10 shadow-pad buttons 304 and their association with keypad buttons 302 in memory 106,
11 processing unit 104 is able to determine that "7" was the intended character. Processing unit
12 104 stores the intended character "7" in memory 106. If however the user fails to select any
13 keypad button 302 after a predetermined amount of time, or the user inputs a "cancel" at any
14 time, then processing unit 104 clears memory 106 of the instance of shadow-pad 303 with its
15 shadow-pad buttons 304 and stops the process.

16
17 [0044] Processing unit 104 generates a new instance of shadow-pad 303 with its
18 shadow-pad buttons 304, and replaces the previous instance of shadow-pad 303 with the new
19 instance of shadow-pad 303 in memory 106. The shadow-pad buttons 304 in this instance of
20 shadow-pad 303 are randomly arranged such that the arrangement of the characters presented
21 by shadow-pad buttons 304 will be different to the previous instance of shadow-pad 303. Each
22 shadow-pad button 304 of this instance of shadow-pad 303 is associated with one keypad
23 button 302 of keypad 301.

24
25 [0045] When secure means 102 is reapplied and a secure channel is detected,
26 processing unit 104 displays this new instance of shadow-pad 303 with its shadow-pad buttons
27 304 and its associated keypad buttons 302 of keypad 301 on display unit 101 as shown in
28 figure 4(e). Shadow-pad button 304 bearing the character "5" associated with keypad button
29 302 bearing the character "4" indicates to the user that to enter the intended character "4",
30 once secure means 102 is removed, the user would have to select keypad button 302 bearing
31 the character "5".

32
33 [0046] Once secure means 102 is removed, input unit 103 displays only keypads 301
34 and its keypad buttons 302 as shown in figure 4(f). Shadow-pads 303 and its shadow-pad
35 buttons 304 are not displayed once secure means 102 is removed. The user selects keypad

1 button 302 bearing the character "5". Based on the stored instance of shadow-pad 303 with its
2 shadow-pad buttons 304 and their association with keypad buttons 302 in memory 106,
3 processing unit 104 is able to determine that "4" was the intended character. Processing unit
4 104 stores the intended character "4" in memory 106. If however the user fails to select any
5 keypad button 302 after a predetermined amount of time, or the user inputs a "cancel" at any
6 time, then processing unit 104 clears memory 106 of the instance of shadow-pads 303 and
7 stops the process.

8
9 [0047] Processing unit 104 can then retrieve the intended characters "3" "7" "4" from
10 memory 106 and send to output unit 105, which can be used for authentication against the
11 user's password for performing a variety of tasks, such as unlocking a device, activating a
12 password manager, accessing a user account, or making a payment.

13
14 [0048] Therefore, although the user's password is "3" "7" "4", the keypad buttons 302
15 that the user actually selects bear the characters "7" "0" "5", masking the user's password from
16 any onlooker. Further, due to the random nature of the arrangement of the characters
17 presented by shadow-pad buttons 304 in each instance of shadow-pad 303, the next time the
18 user logs into system 100, the keypad buttons 302 that the user selects would be different.

19
20 [0049] The embodiment of this invention therefore leverages on a temporary secure
21 channel, which prompts the user which keypad button 302 to select to enter his/her password,
22 when secure means 102 is removed. The advantages are apparent. The invention does not
23 require its users to perform any mental calculations or remember anything beyond the original
24 passwords during password entry. In comparison, many existing innovations impose a
25 considerable amount of cognitive workload on its users. With this invention, the user does not
26 actually key in his password. Therefore, an onlooker would be unable to discern the password
27 (although the onlooker would be able to discern the length of the password). One skilled in the
28 art will appreciate that this invention can be implemented on any portable handheld device, or
29 any automated teller machine or any computer terminal or the like.

30
31 [0050] Figure 5 describes a flowchart illustrating the method in accordance with a
32 preferred embodiment.

33
34 [0051] In step 501, user enters the login screen. User has a password having n
35 characters where n is a number which is larger than one.

1 [0052] In step 502, processing unit 104 generates an instance of shadow-pad 303 with
2 its shadow-pad buttons 304 and stores this instance of shadow-pad 303 in memory 106.
3 Shadow-pad 303 with its shadow-pad buttons 304 are essentially a randomly re-shuffled
4 version of keypad 301 and its keypad buttons 302 such that the characters presented by
5 shadow-pad buttons 304 are non-sequential and random in nature. Each shadow-pad button
6 304 of this instance of shadow-pad 303 is associated with one keypad button 302 of keypad
7 301. This association is also stored in memory 106.

8
9 [0053] In step 503, processing unit 104 detects that secure means 102 has been applied
10 and a secure channel is active.

11
12 [0054] In step 504, processing unit 104 retrieves the instance of shadow-pad 303 with
13 its shadow-pad buttons 304 from memory 106 and displays this instance of shadow-pad 303
14 with its shadow-pad buttons 304 and its associated keypad buttons 302 of keypad 301 on
15 display unit 101.

16
17 [0055] In step 505, processing unit 104 detects that secure means 102 has been
18 removed and a secure channel is no longer active.

19
20 [0056] In step 506, input unit 103 displays keypad 301 and its keypad buttons 302 for
21 the user to select. Shadow-pads 303 and its shadow-pad buttons 304 are not displayed once
22 secure means 102 is removed.

23
24 [0057] In step 507, processing unit 104 processes the user's keypad button 302
25 selection and based on the stored instance of shadow-pad 303 with its shadow-pad buttons 304
26 and its association in memory 106, processing unit 104 is able to determine the intended
27 character (the character the user intended to input).

28
29 [0058] In step 508, processing unit 104 stores the intended character into memory 106
30 and lodges this as a password character entry.

31
32 [0059] In step 509, processing unit 104 checks whether the number of intended
33 characters stored in memory 106 is smaller than n .

34
35 [0060] If the number of intended characters stored in memory 106 is smaller than n ,
36 steps 502, 503, 504, 505, 506, 507, 508 and 509 are repeated.

1 [0061] If the number of intended characters stored in memory 106 is not smaller than n ,
2 in step 510, processing unit 104 sends the stored intended characters to output unit 105.

3
4 [0062] In an alternative embodiment, if input unit 103 is capable of accepting voice
5 input, after step 504, when the instance of shadow-pad 303 with its shadow-pad buttons 304
6 and its associated keypad buttons 302 of keypad 301 are displayed on display unit 101, the
7 user does not need to wait for the secure means 102 to be removed in step 505 to provide the
8 voice input and enter his password. The user simply needs to speak the character presented on
9 shadow-pad button 304 associated with keypad button 302 bearing the intended character.

10
11 [0063] Till this point, the disclosure in the specification has described that each
12 shadow-pad button 304 is associated with one keypad button 302. In an alternative
13 embodiment, one keypad button 302 can be associated with a plurality of shadow-pad buttons
14 304. As shown in figure 6, keypad button 302 is associated with shadow-pad button 304 and
15 shadow-pad button 304'. Keypad button 302 bears the character "A", shadow-pad button 304
16 bears the character "2" and shadow-pad button 304' bears the character "D". Shadow-pad
17 button 304 and shadow-pad button 304' have different graphics to indicate its association with
18 keypad button 302. Shadow-pad button 304 has a "shadow-like" effect graphic that arches
19 downwards while shadow-pad button 304' has a "shadow-like" effect graphic that arches
20 upwards. The obvious advantage is that more shadow-pad buttons 304 may be shown on the
21 screen. With the limited size of most hand held devices, this embodiment of the invention
22 could be particularly useful.

23
24 [0064] One possible use of keypad button 302 having a plurality of associated shadow-
25 pad buttons 304 would be to represent different permutations of the character presented by
26 keypad button 302. For example, using the illustration as provided in figure 6, shadow-pad
27 button 304' may indicate to the user that to enter the uppercase permutation of the intended
28 character "A", once secure means 102 is removed, the user would have to select keypad button
29 302 bearing the character 'D'. And shadow-pad button 304 may indicate to the user that to
30 enter the lowercase permutation of the intended character "a", once secure means 102 is
31 removed, the user would have to select keypad button 302 bearing the character '2'.

32
33 [0065] As the screen size of display unit 101 may be limited, keypad 301 may not be
34 able to be displayed on display unit 101 in its entirety. In such a scenario, in step 701 in figure
35 7, processing unit 104 partitions keypad 301 into a plurality of partitioned keypads 801, 802,

803 (as shown in figure 8). This plurality of partitioned keypads 801, 802, 803 form a keypad pool and this keypad pool is saved to memory 106.

[0066] In step 702, processing unit 104 creates shadow-pad 303 with its shadow-pad buttons 304. Shadow-pad 303 and its shadow-pad buttons 304 are essentially a random re-shuffled version of keypad 301 and its keypad buttons 302. Each shadow-pad button 304 of shadow-pad 303 is associated with one keypad button 302 of keypad 301.

[0067] In step 703, processing unit 104 partitions shadow-pad 303 into a plurality of partitioned shadow-pads in a similar manner to partitioned keypads 801, 802, 803 and stores the plurality of partitioned shadow-pads in memory 106.

[0068] In step 704, processing unit 104 detects that secure means 102 has been applied and a secure channel is active.

[0069] In step 705, processing unit 104 randomly selects one of the partitioned keypads 801, 802 and 803 from the keypad pool, and displays the selected partitioned keypad 801 with its keypad buttons 302 and the associated shadow-pad buttons 304 of partitioned shadow-pad on display unit 101.

[0070] In step 706, if the user is unable to locate the password character on any of the keypad buttons 302 of partitioned keypad 801, user can use input unit 103 to select "next" and processing unit 104 removes partitioned keypad 801 from the keypad pool and randomly selects one of the remaining partitioned keypads 802, 803 from the keypad pool, and displays the selected partitioned keypad 803 with its keypad buttons 302 and the associated shadow-pad buttons 304 of partitioned shadow-pad on display unit 101.

[0071] In step 707, if user locates the password character on one of the keypad buttons 302 of partitioned keypad 803, user notes the character as presented (i.e. shadow-pad character) on the associated shadow-pad button 304 of that keypad button 302, and removes the secure means 102.

[0072] In step 708, once processing unit 104 detects that secure means 102 has been removed and a secure channel is no longer active, processing unit 104 displays partitioned keypad 801 and its keypad buttons 302 on display unit 101.

1 [0073] In step 709, if the user is unable to locate the shadow-pad character on any of
2 the keypad buttons 302 of partitioned keypad 801, user can use input unit 103 to select “next”
3 and processing unit 104 displays partitioned keypad 802 and its keypad buttons 302 on display
4 unit 101.

5
6 [0074] In step 710, if user locates the shadow-pad character on one of the keypad
7 buttons 302 of partitioned keypad 802, user selects that keypad button 302. Processing unit
8 104 then processes the user's keypad button 302 selection and based on the stored shadow-pad
9 303 with its shadow-pad buttons 304 and their association with keypad buttons 302 in
10 memory 106, processing unit 104 is able to determine the intended character (the character the
11 user intended to input).

12
13 [0075] To avoid the inconvenience of scrolling through the numerous partitioned
14 keypads 801, 802, 803 during password entry, the user may choose to customize a keypad
15 which includes all the user's password characters such that the customized keypad and
16 shadow-pad 303 can always fit into display unit 101. The customized keypad will contain a
17 subset of the characters of the entire keypad 301 but all the user's password characters. The
18 shadow-pad 303 in this case will contain a random permutation of the characters of the entire
19 keypad 301. The password entry process with the customized keypad is similar to the process
20 with keypad 301 except that when a secure channel is detected, the customized keypad is
21 displayed; instead of keypad 301 or partitioned keypad 801, 802, 803. The apparent advantage
22 of customized keypad is that it is very convenient for the user to provide the password entry.

23
24 [0076] Throughout the disclosure in the specification, it is described that a user
25 primarily provides input (or inputs his password) by selecting keypad button 302 on keypad
26 301. However, a person skilled in the art would appreciate that a user can provide input via
27 other means (for example, via voice input) and the invention would still be able to function.
28 Voice input may be necessary because the user may be using a wearable device (such as
29 Google glass) and may not have touch screens for inputting passwords. In such an
30 embodiment, display unit 101 is an optical head mounted display of the wearable device. Due
31 to the close proximity of the display unit 101 with the user's eyes, an inherent secure channel
32 will already be in place and there would not be any need for secure means 102. Onlookers will
33 be unable to view whatever is being displayed on display unit 101. With this permanent secure
34 channel in place (permanent as long as the user is wearing the wearable device), display unit
35 101 can display shadow-pad 303 with its shadow-pad buttons 304 and its associated keypad

1 buttons 302 of keypad 301 when the user provides voice input to input unit 103. In this
2 embodiment, input unit 103 comprises a voice recognition device.

3
4 [0077] Figure 9 shows a flowchart describing an embodiment of the invention using a
5 wearable device as described above. In step 901, user enters the login screen. User has a
6 password having n characters where n is a number which is larger than one.

7
8 [0078] In step 902, processing unit 104 generates an instance of shadow-pad 303 with
9 its shadow-pad buttons 304 and stores this instance of shadow-pad 303 in memory 106.
10 Shadow-pad 303 with its shadow-pad buttons 304 are essentially a randomly re-shuffled
11 version of keypad 301 and its keypad buttons 302 such that the characters presented by
12 shadow-pad buttons 304 are non-sequential and random in nature. Each shadow-pad button
13 304 of this instance of shadow-pad 303 is associated with one keypad button 302 of keypad
14 301. This association is also stored in memory 106.

15
16 [0079] In step 903, processing unit 104 detects that secure means 102 has been applied
17 and a secure channel is active. In this embodiment, secure means 102 has been applied
18 because the user is wearing the wearable device with its optical head mounted display in close
19 proximity with the user's eyes.

20
21 [0080] In step 904, processing unit 104 retrieves the instance of shadow-pad 303 with
22 its shadow-pad buttons 304 from memory 106 and displays this instance of shadow-pad 303
23 with its shadow-pad buttons 304 and its associated keypad buttons 302 of keypad 301 on
24 display unit 101.

25
26 [0081] In step 905, processing unit 104 receives the user's selection via voice input.
27 The user speaks the character presented on shadow-pad button 304 associated with keypad
28 button 302 bearing the intended character. Input unit 103 (which comprises a voice
29 recognition device in this embodiment) will receive the voice input as provided by the user.

30
31 [0082] In step 906, processing unit 104 processes the user's selection and based on the
32 stored instance of shadow-pad 303 with its shadow-pad buttons 304 and their association with
33 keypad buttons 302 in memory 106, processing unit 104 is able to determine the intended
34 character (the character the user intended to input).

35
36 [0083] In step 907, processing unit 104 stores the intended character into memory 106.

1
2 [0084] In step 908, processing unit 104 checks whether the number of intended
3 characters stored in memory 106 is smaller than n .

4
5 [0085] If the number of intended characters stored in memory 106 is smaller than n ,
6 steps 902, 903, 904, 905, 906, 907 and 908 are repeated.

7
8 [0086] The "permanent secure channel" embodiment described in figure 9 differs from
9 the "temporary secure channel" embodiment described in figure 5 in the sense that as a
10 permanent secure channel exists, the display unit 101 can display shadow-pad 303 with its
11 shadow-pad buttons 304 and its associated keypad buttons 302 of keypad 301 without any
12 concern of an onlooker glancing upon it, and therefore the user can freely provide his voice
13 input. For the "temporary secure channel" embodiment described in figure 5, once the secure
14 channel is removed, display unit 101 can no longer display shadow-pad 303 with its shadow-
15 pad buttons 304.

16
17 [0087] In the application, unless specified otherwise, the terms "comprising",
18 "comprise", and grammatical variants thereof, intended to represent "open" or "inclusive"
19 language such that they include recited elements but also permit inclusion of additional, non-
20 explicitly recited elements.

21
22 [0088] It will be apparent that various other modifications and adaptations of the
23 application will be apparent to the person skilled in the art after reading the foregoing
24 disclosure without departing from the spirit and scope of the application and it is intended that
25 all such modifications and adaptations come within the scope of the appended claims.

1 **CLAIMS**

2

3 1. A system for accepting entry of a password, the password comprising at least one
4 password character, the system comprising:

5 a display unit;

6 a secure means controlled by a user and adapted to display a secure channel on the
7 display unit visible only to a user providing a user entry, the secure channel being removed
8 upon deactivation of the secure means;

9 a processing unit configured to generate a plurality of randomly arranged shadow-pad
10 buttons interposed with a plurality of keypad buttons, each one of the plurality of keypad
11 buttons bearing a keypad character, and each one of the plurality of shadow-pad buttons
12 bearing a shadow-pad character, and each one of the plurality of shadow-pad buttons being
13 associated with one of the plurality of keypad buttons;

14 a memory unit for storing the plurality of shadow-pad buttons interposed with the
15 plurality of keypad buttons; and

16 an input unit for accepting the user entry upon the removal of the secure channel;

17 wherein the processing unit is further configured to display on the display unit the
18 plurality of shadow-pad buttons interposed with the plurality of keypad buttons upon the
19 implementation of the secure channel, each one of the plurality of shadow-pad buttons having
20 a visual effect to indicate the association with one of the plurality of keypad buttons;

21 wherein the at least one password character matches the keypad character of one of the
22 plurality of keypad buttons, the shadow-pad character of the shadow-pad button associated
23 with the matched keypad button indicates that the shadow-pad character should be selected as
24 the user entry upon the removal of the secure channel; and

1 wherein the processing unit is further configured to recognize that the at least one
2 password character has been entered when the shadow-pad character is entered as the user
3 entry.

4

5 2. The system of claim 1 further comprising an output unit, wherein the processing unit
6 is further configured to send the at least one password character to the output unit for
7 authentication.

8

9 3. The system of claim 1 or claim 2 wherein the secure means is a hand-shielding gesture
10 over a gesture detection area.

11

12 4. The system of claim 1 wherein at least one of the plurality of keypad buttons has a
13 plurality of associated shadow-pad buttons.

14

15 5. The system of claim 1 wherein the display unit, processing unit, memory unit and
16 input unit are part of a portable handheld device or an automated teller machine or a computer
17 terminal.

18

19 6. The system of claim 1 wherein the shadow pad character is selected either by touching
20 a keypad button or by voice input received by the input unit.

21

22 7. A method for accepting entry of a password, the password comprising at least one
23 password character, the method comprising the steps of:

24 generating with a processing unit, a plurality of randomly arranged shadow-pad
25 buttons interposed with a plurality of keypad buttons, each one of the plurality of keypad
26 buttons bearing a keypad character, and each one of the plurality of shadow-pad buttons

- 1 bearing a shadow-pad character, and each one of the plurality of shadow-pad buttons being
2 associated with one of the plurality of keypad buttons;
3 storing the plurality of shadow-pad buttons interposed with the plurality of keypad
4 buttons;
5 implementing with a secure means controlled by a user a secure channel for a display
6 unit such that the display unit is visible only to the user providing a user entry;
7 displaying on the display unit, the plurality of shadow-pad buttons interposed with the
8 plurality of keypad buttons, each one of the plurality of shadow-pad buttons having a visual
9 effect to indicate the association with one of the plurality of keypad buttons;
10 wherein the at least one password character matches the keypad character of one of the
11 plurality of keypad buttons;
12 removing the secure channel by deactivating the secure means;
13 accepting the user entry with an input unit, the user entry being the shadow-pad
14 character of the shadow-pad button associated with the matched keypad button; and
15 recognizing with the processing unit, that the at least one password character has been
16 entered.
17
18 8. The method of claim 7 further comprising the step of sending with the processing unit,
19 the at least one password character to an output unit for authentication.
20
21 9. The method of claim 7 wherein the step of implementing a secure channel with a
22 secure means comprises the step of placing a hand-shielding gesture over a gesture detection
23 area.
24
25 10. A wearable device for accepting entry of a password when worn on a user's head, the
26 password comprising at least one password character, the wearable device comprising:

1 an optical head mounted display;
2 a processing unit configured to generate a plurality of randomly arranged shadow-pad
3 buttons interposed with a plurality of keypad buttons, each one of the plurality of keypad
4 buttons bearing a keypad character, and each one of the plurality of shadow-pad buttons
5 bearing a shadow-pad character, and each one of the plurality of shadow-pad buttons being
6 associated with one of the plurality of keypad buttons;
7 a memory unit for storing the plurality of shadow-pad buttons interposed with the
8 plurality of keypad buttons; and
9 a voice recognition device for processing a voice input from the user;
10 wherein the processing unit is further configured to display on the optical head
11 mounted display the plurality of shadow-pad buttons interposed with the plurality of keypad
12 buttons, each one of the plurality of shadow-pad buttons having a visual effect to indicate the
13 association with one of the plurality of keypad buttons;
14 wherein the at least one password character matches the keypad character of one of the
15 plurality of keypad buttons, the shadow-pad character of the shadow-pad button associated
16 with the matched keypad button indicates that the shadow-pad character should be selected as
17 the voice input; and
18 wherein the processing unit is further configured to determine that the at least one
19 password character has been entered when the shadow-pad character is entered as the voice
20 input.

21
22 11. The wearable device of claim 10 wherein at least one of the plurality of keypad buttons
23 has a plurality of associated shadow-pad buttons.

12. A method for accepting entry of a password with a wearable device when worn on a user's head, the password comprising at least one password character, the method comprising the steps of:

generating with a processing unit of the wearable device, a plurality of randomly arranged shadow-pad buttons interposed with a plurality of keypad buttons, each one of the plurality of keypad buttons bearing a keypad character, and each one of the plurality of shadow-pad buttons bearing a shadow-pad character, and each one of the plurality of shadow-pad buttons being associated with one of the plurality of keypad buttons;

storing the plurality of shadow-pad buttons interposed with the plurality of keypad buttons into a memory unit of the wearable device;

displaying on an optical head mounted display of the wearable device, the plurality of shadow-pad buttons interposed with the plurality of keypad buttons, each one of the plurality of shadow-pad buttons having a visual effect to indicate the association with one of the plurality of keypad buttons; wherein the at least one password character matches the keypad character of one of the plurality of keypad buttons;

accepting a voice input from the user with a voice recognition device of the wearable device, the voice input being the shadow-pad character of the shadow-pad button associated with the matched keypad button; and

determining with the processing unit, that the at least one password character has been entered.

[21] 20/1

▲ IPEA