IMPROVED SYSTEM AND METHOD FOR RANDOM ENTRY OF PASSWORD

TECHNICAL FIELD

The present invention relates to an improved system which assigns an incomplete password each time an user is to access a secured system employing a security code/PIN/password entry system, so that to an observer, the password is entered in a random manner.

BACKGROUND ART

The current security code/ PIN entry pad system is highly insecure and is especially prone to shoulder-surfing attacks. An attacker can easily decipher the password by watching a user's finger movement from a moderate distance. With the help of powerful optical devices such as mini hidden camera, binoculars or even a camera phone, the finger movement of user can be recorded and analyzed in detail to obtain the user's security code/ PIN. In the case of ATM card, once attacker is confident of a good guess of the PIN, theft or robbery would shortly follow to seize the card.

Some user may use a very long security code/PIN to deter attackers; however, this method is not only stressful on user's memory, it is also futile if attackers can record the entire entry process.

Extensive study has also been done on graphical password schemes which are believed to be more secure and resilient to dictionary attacks compared to textual passwords; however, graphical password might also be more vulnerable to shoulder-surfing attacks[1-2].

---

[1] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, The Design and Analysis of Graphical Passwords. In the 8th USENIX Security Symposium, 1999.

[2] H. Tao, Graphical password authentication arrangement for computer, displays grid with multiple horizontal nd vertical lines, Patent No. CA2495445-A129, Filed 29 Jan. 2005, In Derwent Innovations Index.

In one graphical password scheme, binary pressure entry was proposed as an invisible user input to thwart shoulder-surfing attacks [3].

Although such scheme may be effective to certain extend, its may also be rather memory taxing if we are required to also remember the pressure we use, not to mention the large number of password we need to memorize.

There is also another form of security attack done by keylogger program or device. Such program records all data entry from the user and sends this information to the attacker via email or other means. From the data entry records, attacker just needs to do some analysis of the information to obtain good guesses to the password. This form of attack is more commonly experienced by users using online password entry system found in email, blog, online games etc.

Therefore, a good password scheme should be able to provide resistance to dictionary attack, shoulder-surfing attack and keylogger attack. On top of these criteria, the password should be easily to memorize, password entry process should be simple and the cost of implementation should also be minimal.

With all the above points in mind, we proposed our novel password scheme. In our scheme, we do not require user to enter the entire password at all. The key to our invention is entering an incomplete password in what seems like a totally random order (to someone observing the user as the user enters the password or to someone monitoring the key strokes of the user as the user enters the password).

It is possible to have the user of the password enter an incomplete password in what seems like a totally random order (to someone observing the user as the user enters the password or to someone monitoring the key strokes of the user as the user enters the password).

---

[3] A Patent application on "Shoulder Surfing Resistant Graphical Password with Haptics", submitted to the TTBE, university of Ottawa, October 2005

SUMMARY OF INVENTION

The object of the invention is to enter an incomplete password in a totally random order each time the user uses the password. For example, if the correct password memorized by the user is "789012". Using an ATM system as an example, upon swiping the card, the user will be shown 6 blanks spaces (there are 6 characters in the password) with some of the spaces filled up with asterisk. If 2 of the spaces are randomly chosen and filled with asterisk, the user just need to enter the remaining 4 characters to the blanks. The order of entering the 4 remaining characters will be randomly chosen by the blinking underscore shown on the user interface.

A further object of the invention is to enter the required password using a touch screen keypad with characters of the keypad displayed in different orientation on the user screen. The characters can be alphanumeric or symbols. The positioning of the characters is not entirely random and should be positioned in an ordered manner such that it is easy for user to find and enter the character. For example, if the characters are numeric, the numbers should be positioned in sequence next to each other and each time a user access the system, the sequence of number should vary, either ascending or descending and also in different directions. In this way, there will not be any character of the keypad with a fixed position on the keypad and it would be extremely difficult for attacker to decipher the password by just analyzing user's finger movement without getting a clear look of the user screen to find out the exact position of each character. In other words, unless an attacker has a clear and direct view of the user screen to tell him/her where the characters are positioned, is would be nearly impossible to guess the correct password just from analyzing user's finger movement. The purpose of positioning the characters of the keypad in an ordered manner as oppose to random positioning is to make the keypad more user-friendly.

DETAILED DESCRIPTION OF DRAWINGS

For a better understanding of the invention, its advantages, and the objects attained by its use, reference should now be made to the accompanying drawings. The accompanying drawings illustrate one or more embodiments of the invention and together with the description herein, serve to explain the workings and principles of the invention.

Figure 1 is a flow diagram of how the program code will generally run in the case of an ATM machine.

Figure 2 shows an example of the blanks generated by step 103. M number of blanks are randomly selected and filled with asterisk. In this case, M = 2. One of the remaining unfilled blanks are randomly selected and prompted for user input. In this case, the blank at the 4th character position is selected and is prompting for a user input using the blinking underscore.

Figure 3- 10 show the different positioning of the characters of the keypad used in a touch screen as proposed in this invention. These positionings assume that numeric characters are used as input. The positions of the characters are changed in each of the Figure. However, the characters are still arranged in an ordered manner or have some sequence or order. The positioning of the characters of the keypad in the touchscreen is not entirely random.

DETAILED DESCRIPTION OF INVENTION

The proposed password scheme may be applied to all security code/ PIN/ password entry system. For easy discussion, we will use an ATM system to illustrate and explain our invention. In the first embodiment, an ATM machine has a fixed data entry pad and a screen. The screen will show the blanks representing the alphanumeric characters of the password to be entered.

As shown in Figure 1, when a card is swiped or entered into the ATM machine, a card verification process 101 will be performed to determine if a card is valid. The verification process can be a simple check of the expiry date or by the embedded image technology mentioned by U.S. Patent 6321981 or the established verification process used by current ATM technology. If card is invalid, the card will be ejected 102. If card is valid, the password length N will be determined by 103 and N blanks will be generated as shown in Figure 2. The password length N can be fixed for all customers, for example N=6 for most banks in Singapore, or defined by user. N may either be determined from hidden card information or from bank database.

After the blanks are generated, we move on to step 104 where M of the blanks are randomly chosen and filled up with asterisks as shown in Figure 2. In order to ensure that someone who picks up an ATM card by chance will less than or equal to 0.03% probability of guessing the right password or PIN in 3 attempts, the number of unfilled blanks (N-M) should be greater than or equal to 4 (Bank of America uses 4-digit PIN currently). Hence, if N=6, M can either be 1 or 2 but never 0.

Step 105 will randomly selected one of the unfilled blanks and prompt the user for input. The prompting process can be done using blinking underscore as shown in Figure 2. Alternatively, the prompting process could be done through other means such as arrow pointing towards a selected unfilled blank or flashing a selected unfilled blank. For ATM machines using color screens, the selected unfilled blank could be of a different color to prompt the user for input at that position.

The input from user may be any form of characters or symbol. However, for purpose of illustration only, we use digits from 0-9. The input to each of the blanks will be displayed as asterisk like other pre-filled blanks in step 104. After a user had entered an input for a blank, another unfilled blank will be randomly selected until all the blanks are filled up.

After all the unfilled blanks are filled up and the "ACCEPT" or "ENTER" key is activated as shown in the flow diagram, the password verification process 106 will commence. The verification process will only verify the user inputs to make sure that both the positions and characters entered exactly match the correct password. The pre-filled asterisks will not be checked. In other words, assuming the correct password is "789012" and the first randomly chosen blank is the 4th blank, a "0" has to be entered to be valid and if the next randomly chosen blank is the 1st blank and then the 5th blank, a "7" followed by a "1" have to be entered to be valid. The entire process of entering four unfilled blanks would lead to the user entering the numbers "0", "7", "1" and finally "9" to complete the entire string in the password " 789012". Invalid password will lead to card ejection 107 and valid password will bring the user to the transaction option page 108.

Using the proposed scheme, it is extremely difficult for attackers to guess the correct password. Firstly, one of the best ways to deter against shoulder-surfing is not to enter the password at all. Hence, in step 104, we purposely add in the asterisk so that user is only required to enter an incomplete password. On top of this, in process 105, the sequence of entering has been purposely jumbled to confuse the attackers. Therefore, even if an attacker observed that a user entered "0719", when the attacker swipe the card, the system might not ask for the same password at all. For instance, in the next access to the system, the system may fill the last 2 blanks with asterisk and require the attacker to fill up the first 4 blanks, which in this case, the correct entry would be "7", "8", "9" and "0" being corrected entered into their respective position. However, the attacker had observed the entering of "0", "7", "1" and finally "9" to complete the entire string in the password. Obviously, in this case, the attacker will never succeed if he sticks to what he observed. Moreover, as both 104 and 105 produce random results, shoulder-surfing attackers may find users entering different sets of password at each login and this is absolutely confusing for the attackers. Moreover, if we allow M in 104 to vary, the number of characters a user enters may also differ at each login or access.

In fact, if we increase N to maybe 10, step 104 and 105 will make the job of shoulder-surfing attacker exponential tedious (M may be 1, 2, 3, 4, 5 or 6) and may even render shoulder-surfing an obsolete threat in future.

In addition, if our password length is long enough, say 10 characters, step 104 and 105 will help to ensure that we almost always enter a different password at each login. This would pose a natural resistance to keylogger attacks as there would not be a fixed sequence of characters we keep entering.

An additional benefit of such scheme is user may actually use the same password for a few of his or her accounts as what he or she enters at each login is almost always different and never a complete password (M never equal 0). Memorizing just 1 or 2 longer passwords is definitely a much easier task than the multiple passwords that we need to memorize for each of our different accounts currently.

In the second embodiment, we will use an ATM machine with a touch screen keypad. The position of the characters on the keypad is changed each time a

user login. The characters on the keypad are not shuffled randomly; instead, the characters are arranged in an ordered sequence as shown in Figure 3-10. The purpose of this scheme is to change the position of the characters on the keypad as shown on the touch screen to deter shoulder-surfing attacks and at the same time keeping this scheme as user friendly as possible to speed up transaction. Other arrangements of the character positions such as arranging the characters in a clockwise or counter-clockwise fashion or some ordered manner are also possible and within the scope of the invention.

After the card verification process 101 in Figure 1, if card is valid, a possible keypad arrangement could be randomly chosen from a list and displayed. For example, Figure 4 keypad character arrangement could be chosen and at the next access of the system by either the same or different user, Figure 10 could be chosen. A list of user friendly keypad arrangement could be stored in the ATM and the system will randomly assign one at each login. In this way, it would be almost impossible for shoulder-surfing attackers to guess the password from user's finger movement unless the attacker has a clear view of the user screen and knows the positioning of the characters.

While an embodiment of the invention have been described, it should be apparent, however, that various modifications, rearrangements, substitutions alterations and adaptations to those embodiments may occur to persons skilled in the art with the attainment of some or all of the advantages of the present invention. Accordingly, it should be clearly understood that the present invention is not intended to be limited by the particular features and structures hereinbefore described and depicted in the accompanying drawings. It is therefore intended to cover all such modifications, alterations and adaptations without departing from the scope and spirit of the present invention as defined by the appended claims.

ADVANTAGEOUS EFFECTS OF THE INVENTION

The system and method of a randomly entered password would make it very difficult for someone who is shoulder surfing to guess the correct password.

The system and method of a randomly entered password would also make it very difficult for any key logging program to capture the correct password because the entire password is not entered in the first instance and secondly the characters requested by the system are randomly assigned.

The same password can be used for multiple accounts and attackers will not even notice since different characters or character order are entered by the user at each login. This system helps to reduce the number of passwords an user is required to remember in his or her lifetime.

The system and method of a randomly entered password using a touch screen with a keypad showing the characters of the keypad in an ordered manner but not in the conventional order of a numeric keypad would make it extremely difficult to guess what number is being entered and for which position of the password.

CLAIMS

1. A system for an improved password for all security code/PIN/password entry system, the system operable with a display screen for entry of password, and a keypad for entering the security code/PIN/password wherein an user is required to enter his personal password before being allowed to enter into the system and wherein the user has to enter an incomplete password in a totally random order each time the user uses the password.

2. The system as claimed in Claim 1 wherein the user will be shown N blanks spaces (there being N characters in the password) with some of the spaces are randomly filled up with asterisk for which no data entry is required and the user is required to enter the remaining characters of the password through a prompting means when prompted by the system by correctly entering each character corresponding to the position of the password prompted by the system and wherein the order of entering the remaining characters of the password will be randomly chosen by the system through use of such prompting means.

3. A system for an improved password for all security code/PIN/password entry system, the system operable with a display screen which is a touch screen, and a keypad for entering the security/PIN/password is displayed on the touch screen, wherein an user is required to enter his personal password before being allowed to enter into the system and wherein the user has to enter an incomplete password in a totally random order each time the user uses the password.

4. The system as claimed in Claim 3 wherein the user will be shown N blanks spaces (there being N characters in the password) with some of the spaces are randomly filled up with asterisk for which no data entry is required and the user is required to enter the remaining characters of the password through a prompting means when prompted by the system by correctly entering each character corresponding to the position of the password prompted by the system and wherein the key pad for entry of characters for the password is displayed in an

ordered manner and the order of entering the remaining characters of the password will be randomly chosen by the system through use of such prompting means.

5. The ordered manner of the keypad as claimed in Claim 4 being a keypad arranged in an ordered diagonal manner across the touch screen.

6. The ordered manner of the keypad as claimed in Claim 4 being a keypad arranged in an ordered vertical manner across the touch screen.

7. The ordered manner of the keypad as claimed in Claim 4 being a keypad arranged in an ordered horizontal manner across the touch screen.

8. The ordered manner of the keypad as claimed in Claim 4 being a keypad arranged in any other ordered manner across the touch screen.

9. The prompting means as claimed in Claim 2 or Claim 4 being a blinking underscore shown on the user interface.

10. The prompting means as claimed in Claim 2 or Claim 4 being a highlighted blank shown on the user interface.

11. The prompting means as claimed in Claim 2 or Claim 4 being an arrow displayed next to the blank to be entered on the user interface.

12. A method for an improved password for all security code/PIN/password entry system, wherein an user have to enter his personal password before being allowed to enter into the system wherein the user has to enter an incomplete password in a totally random order each time the user uses the password.

13. The method as claimed in Claim 12 wherein the user will be shown N blanks spaces (there being N characters in the password) with some of the spaces are randomly filled up with asterisk for which no data entry is required and the user is required to enter the remaining

characters of the password through a prompting means when prompted by the system by correctly entering each character corresponding to the position of the password prompted by the system and wherein the order of entering the remaining characters of the password will be randomly chosen by the system through use of such prompting means.

14. The system for an improved password for all security code/PIN/ password entry system as claimed in Claim 1 or Claim 3, said system being used for carrying financial transactions.

15. The system for an improved password for all security code/PIN/ password entry system as claimed in Claim 1 or Claim 3, said system being used for carrying banking transactions.

16. The system for an improved password for all security code/PIN/ password entry system as claimed in Claim 1 or Claim 3, said system being used for carrying payment transactions.

17. The system for an improved password for all security code/PIN/ password entry system as claimed in Claim 1 or Claim 3, said system being used for carrying credit card transactions.

18. The system for an improved password for all security code/PIN/ password entry system as claimed in Claim 1 or Claim 3, said system being used for carrying debit card transactions.