ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 2; Page No. 01-07

On Screen Randomized Keyboard with Virtual Password Functions

Neenu N A[1], Sruthy Manmadhan[2]

[1]PG Scholar, Dept. of Computer Science and Engineering, NSS College of Engineering, Palakkad, Kerala

Email: neenu.na.89@gmail.com

[2]Assistant Professor, Dept. of Computer Science and Engineering, NSS College of Engineering, Palakkad, Kerala

Email: sruthym.88@gmail.com

ABSTRACT

Online banking has become increasingly popular globally because it is so easy and convenient for the internet users to manage their bank accounts from anywhere of the world at any time. The internet improves the user's banking experience as he can access his account and handles all his financial needs from anywhere without going to the branch office using his computer connected to the internet. Online banking user's faces various security risks such as brute force attacks, key logging attacks, shoulder surfing attacks, etc. The design of secure authentication protocols is quite challenging, considering that software installed in PCs to observe the user's behavior and to capture the credentials, thus making the PCs untrusted devices. Involving human in authentication protocols is also difficult as they have limited computation capability and memorization. Therefore relying on users to enhance security will reduces the usability. The security and usability can be enhanced with the help of some handheld devices like smartphone. In this paper, a password based visual authentication protocol using random keyboard with some special symbols associated with each character is proposed. Also password is made more complex by introducing Virtual Password Functions. Using this new keyboard, users can enter their credentials. This is effective against the key logging attacks and shoulder surfing attacks by increasing the amount of short term memory required in an attack.

Key Words: *Authentication, Smartphone, Malicious code, Keylogger, Shoulder Surfing Attacks (SSA), Differentiated Virtual Passwords, Secret Little Functions*

INTRODUCTION:

The threads against electronic and financial services can be classified into two major classes: credential steading and channel breaking attacks. Credentials such as users identifiers, passwords, PINs, etc. can be stolen by an attacker if they are poorly managed [8]. The channel breaking attacks which allow for eavesdropping on communication between users and a financial institution. While classical channel breaking attacks can be prevented by the proper usage of a security channel such as Internet Protocol Security (IPSec) and SSL (Secure Sockets Layer), recent channel breaking attacks are more challenging. The key logging attacks, session hijacking, phishing and pharming and visual fraudulence cannot be addressed by simply enabling encryption.

The major attacks are the key logging and shoulder surfing attacks. A key logger [1] is software designed to capture all of a user's keyboard strokes and then make user of them to impersonate a user in financial transaction. For example, whenever a user types in her password in a bank's log in box, the key logger intercepts the password. The threat of such key loggers is pervasive and can be present both in personal computers and public systems; there are always cases where it is necessary to perform financial transactions using a public computer although the biggest concern is that a user's credentials are likely to be stolen in these computers. Even worse, key loggers, often root kitted, are hard to detect since they will not show up in the task manager process list. There is high chance of this key logging attack when we are performing the financial transactions using a public computer where the user's password is likely to be stolen by the key logger while the user enters the password. To mitigate the key logger attack, virtual or onscreen keyboard with random keyboard arrangements are widely used in practice. But, since the key logger which has the complete control over the entire pc can easily capture every event and read the videos buffer to create a mapping between the clicks and the new alphabet.

Another major attack is the shoulder surfing attack [2], where the attacker observes the logon procedure by

Corresponding author: Neenu N A

looking over the users shoulder, and tries to recover that users credentials. The advanced SSA like recording attacks using a miniature video camera and a smart phone are crucial. There are many methods dealing with this issue, but most of them are not widely accepted in practice due to various usability problems. Some other methods like Eye-gazed scheme and brain computer interface based scheme require expensive non-standard hardware devices that have not gained sufficient levels of acceptability. All these methods are not providing a successful solution against the shoulder surfing attacks.

An intermediate device that bridges a human user and a terminal is introduced. Instead of user directly invoking the regular authentication protocol, she invokes a more sophisticated user friendly protocol via the intermediate helping device. Each interaction is visualized using a Quick Response (QR) code. And it uses a random blank keyboard with special symbols associated with each key.

1. SECURITY ATTACKS:

There are several security attacks existing in this new era [1].

KEY SPACE AND BRUTE-FORCE ATTACKS

A Brute-Force attack or exhaustive key search cryptographic attack that can be used against any encrypted data. A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN).Such an attack might be utilized when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking possible passwords or keys until the correct one is found. When password guessing, this method is very fast when used to check all short passwords. When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. A brute force attack may also be referred to as brute force cracking.

The following measures can be used to defend against brute force attacks:

- Require users to have complex passwords.
- Limiting the number of times a user can attempt to log in.
- Temporarily locking out users who exceed the specified maximum number of login attempts.

MALWARE (MALICIOUS SOFTWARE)

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, worms, Trojan horses, ransom ware, spyware, adware, scareware, and other malicious programs. Spyware or other malware is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics. An example of such software, which was described as illegitimate, is the Sony rootkit, a Trojan embedded into CDs sold by Sony, which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits, and created vulnerabilities that were exploited by unrelated malware.

Software such as anti-virus, anti-malware, and firewalls are used by home users and organizations to try to safeguard against malware attacks.

KEY LOGGING ATTACKS

Key logger is software that always resides on the terminal with high incentives of breaking the security of the system by tracking the key events. It is a hardware device or small program monitoring each keystroke a user types on a computer’s keyboard. It is sometimes called a system monitor.

As a hardware device, a keystroke logger is a small plug serving as a connector between the user’s keyboard and computer. Because the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user’s behavior—a hacker or a cracker—to physically hide such a device. (It helps that most workstation keyboards plug into the back of the computer.)

Figure 1: Key Logging Attacks

Figure 2: Shoulder Surfing Attacks

As the user types, the hardware device collects each keystroke and saves it as text in its own miniature storage device. Later, the person who installed the keystroke logger can return and remove the device to access the gathered information. A keystroke logger program does not require physical access to the user's computer. It can be downloaded by someone who wants to monitor activity on a particular computer, or it can be downloaded unwittingly as spyware and executed as part of a rootkit or remote administration (RAT) Trojan. The key logger is capable of doing the following:

- While residing in a user's terminal, the attacker can capture the user's credentials such as passwords, a private key and One Time Password (OTP) string.
- The attacker can deceive a user by showing a genuine looking page that actually transfers money to the attacker's account with the captured credentials.
- After a user successfully gets authenticated with a valid credential, the attacker can hijack the authenticated session.

SHOULDER SURFING ATTACKS

In this attack [2], the attacker observes the login procedure by looking over the user's shoulder and tries to recover the user's PIN. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done at long distance with the aid of binoculars or other vision-enhancing devices. The strongest variant of this attack is the Recording attack in which the attacker employs a recording device to record the entire authentication session. The attack without any recording device is called as Human Shoulder Surfing attack. We consider an attacker who shoulder surfs multiple with the user unaware of the attacks. Also someone in a close relationship with a user may observe the procedure used to unlock that user's mobile phone multiple times. After the attacker obtains the information about the correct credentials from shoulder surfing attack, they will try to pass the PIN/password entry test by randomly guessing the missing information.

2. EXISTING SECURITY MECHANISMS:

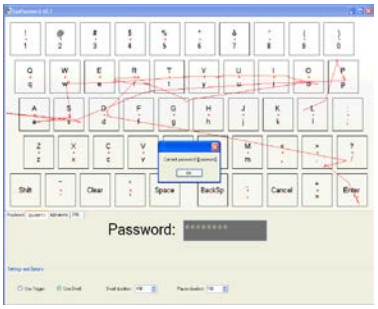

Figure 3: Eye – Gazed Password Entry

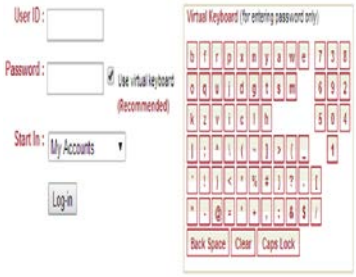

Figure 4: Virtual Keyboard

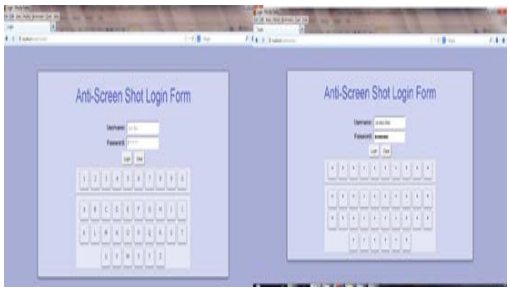

Figure 5: Anti-Screenshot Virtual Keyboard

EYE – GAZED PASSWORD ENTRY

In the eye – gazed password entry method [5] [6], the user enters the password or PIN by selecting from an onscreen keyboard using only the orientation of their eye pupils. That is using the position of their eye gaze on the screen keyboard. Each key has a bright red dot at the center of it. The focus point allows the user to focus their gaze at the center of the target for increasing the accuracy of eye tracking data. This method is resistant against the shoulder surfing attacks. But this method does not provide the user with appropriate feedback that a key press has indeed the correct one or not. Additional

hardware components are needed for sensing the eye movement. Example: password is: **password.**

This system is resistant against Key logging attacks and shoulder surfing attacks. But it is not user friendly. Also it requires costly sensors to sense the eye movement of users. It is also difficult to sense the eye movement accurately if the keyboard size is small.

VIRTUAL KEYBOARDS

Virtual keyboards [9] are commonly used as on –screen input method in devices with no physical key board where there is no space for one. Like pocket computers, touch screen enabled mobile phones etc. Virtual keyboard can reduce the risk of keystroke logging. It is more difficult for the malware to monitor the display and mouse to obtain the data entered via virtual keyboard.

The advantages of virtual keyboard are it reduces the risk of key logging attacks and it is more difficult for malware to monitor the display and mouse to obtain the data entered via the virtual keyboard. This system has many disadvantages. The first one is that the key logger has the complete control over the entire PC can easily capture every event and read the video buffer to create a mapping between the clicks and the new alphabet. Also the shoulder surfing attack is easier. An observer can typically watch the screen more easily than keyboard. A user may not be able to point and click as fast as they could type on the key board.

ANTI SCREENSHOT VIRTUAL KEYBOARD

In the anti-screenshot virtual keyboard [10], when the mouse move to one key, all the keys on that particular row of the keyboard are changed to some special symbol like an asterisk(*) or a hash(#).When the user clicks a particular button all the keys on the virtual keyboard are changed to some special symbol, say asterisk(*). Hence even if the Trojan takes a screenshot on the mouse click event, all that will be captured is asterisk(*).When the user releases the key, the keyboard is retained back. However, in the above approach, if the Trojan Horse takes the screenshot of the virtual keyboard layout, then it is possible to identify the password. Hence in order to overcome this problem, real time refreshing can be done i.e when the user releases a key, instead of bringing the keyboard back to the original position, its keys can be randomized. However total randomization of the keyboard will make the user uncomfortable.

The anti-screenshot virtual keyboard requires some delayed time of say 0.2 seconds after the mouse button is released to show the values of keys and they are refreshed by areas on the virtual keyboard. Thus it is obvious that efficiency of virtual keyboard is less than that of traditional keyboard.

This anti-screenshot virtual keyboard solves the problem of screen capture by advanced Trojans. But it is less efficient as compared to the traditional keyboard. Also shoulder surfing attacks is possible.

RANDOMIZED ON SCREEN BLANK KEYBOARD

This method [1] uses a password shared between the server and the user and a randomized on screen blank keyboard. This method works as follows:

1. The user connects to the sender and sends his/her ID.
2. The server checks the received ID to retrieve the user's public key from the database. The server prepares a random permutation of keyboard arrangement and encrypts it with the public key retrieved from the database. Then it encodes the cipher text with QR encoder. The server then sends the result with a blank keyboard to the user.
3. In the user's terminal, a QR code is displayed together with a blank keyboard. As the on screen keyboard does not have any alphabets in it, the user cannot input the password. Now the user executes the smart phone application which first decodes the QR code to get the cipher text. The cipher text is then decrypted by the smartphone application with the private key of the user to display the results on the screen of the smartphone.
4. When the user sees the blank keyboard with the QR code through the application on the smartphone that has a private key, alphanumeric appear on the blank keyboard layout and the user can click the proper button for the password. The user clicks his password on its terminal screen while seeing the keyboard layout in the smartphone screen. The terminal does know what the password is, but only knows which buttons are clicked. The identity of the buttons clicked by the user is send to the server by the terminal.
5. The server checks whether the password entered by user is correct or not by confirming if the correct buttons have been clicked.

This method is resistant against Key logging attacks. Also it is resistant against brute force attacks and malicious software attacks. But shoulder surfing attacks is possible.

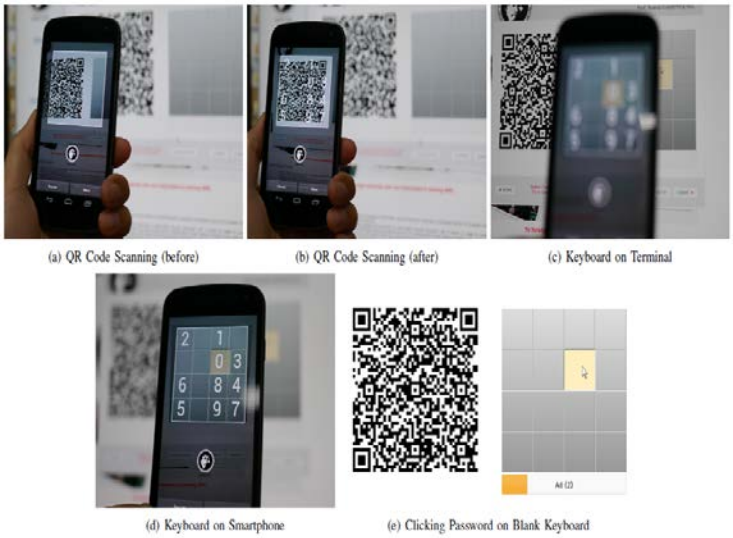

Figure 6: Randomized Blank Keyboard Generation

(a) and (b) show the moments of a QR code scanning of a keyboard layout. (c) shows the blank keyboard shown at the terminal (on LCD screen). (d) shows the decoded randomized layout of the keyboard obtained from the QR code after decryption as viewed on smartphone. Note that the yellow square on which the mouse cursor is hovering in the terminal is shown through the smartphone to assist user's input. (e) shows that a user is clicking the password on the blank keyboard while seeing numbers through the smartphone**.**

3. PROPOSED APPROACH:

Since the randomized on screen blank keyboard method is not resistant against shoulder surfing attacks, it has been extended to include some special symbols along with each character in the blank keyboard [1] [2]. Also the password is made more complex by including virtual password. A new differentiated security mechanism using virtual password scheme ranging from weak security to strong security is proposed. Here user specified functions or programs or secret little functions are used. A virtual password [11] is a dynamic password that is generated differently each time from a virtual password scheme and then submitted to the server for authentication. A differentiated security mechanism for system registration in which the system allows users to choose a registration scheme ranging from the simplest one to a complex one. Users have to choose a virtual password function during the time of registration. A user can choose a virtual password function recommended by the server, define his/her own virtual password function, or even define a common C program to share between the user and the server to calculate the password. Secret Little Functions are the functions or programs specified by the user and it will be kept secret between the user and the server. During registration, user will be specifying a virtual password function. When the user logins, the server provides an input and user have to calculate the virtual password based on that input and append this virtual password with the actual fixed password. The server will also calculate the virtual password and matches with the new password entered by the user. Here in this method, when the user successfully enters the username server will display a barcode and a random keyboard arrangement with special symbols. The barcode contains the key for choosing the keyboard arrangement and also the input value to the virtual password function. When the user scans the qrcode using the mobile application, the app will first calculate the virtual password by applying the input value stored in the qrcode to the virtual password function. After displaying the virtual password in the mobile screen when the user clicks OK, the 4*4 keyboard arrangement with special symbols corresponding to the key specified in the qrcode is displayed. For e.g., if the user specified a simple C program to calculate the factorial of a number, and the server will provide a random number in the qrcode, say 5, after scanning the mobile app will provide the virtual password result as 120. The user then has to append this virtual password to his actual fixed password and has to enter this new password using the below proposed method.

Consider if the PIN or password is having 4 digits. Therefore it needs four rounds to complete the PIN entry. The first round is the session key decision round and the remaining rounds are the PIN entry rounds. This method uses the same steps of generating a randomized blank keyboard using the scanning of the QR code using mobile phone. When the keyboard is displayed in the smartphone, users can identify the position of the first digit of his/her PIN in the blank keyboard in the terminal. He recognizes the symbol at the position of the first digit of PIN as temporary session key. The remaining rounds are the PIN entry rounds in which ith digit of the PIN is entered in the ith round by identifying the positions in the blank keyboard by looking to the smartphone and aligning the recognized session key character to the position of the individual digits on each round. This alignment can be done by dragging and changing the object array. Once the user has completed inputting or aligning the session key of the last digit of the PIN to correct position, the PIN or password entered will be send to the server.

Thus the keylogging attacks and also the shoulder surfing attacks can be prevented because the password is random each time. Also as the mobile app is calculating the virtual password, user need not have to spend much time in calculating the virtual password. Since the keyboard does not contain any numbers or alphabets, shoulder surfing attack is also not possible. Instead of numeric keyboards, we can extend this method to enter alphanumeric characters by using blank alphanumeric keyboard to enter the passwords. We can use this method to enter the passwords to the secured sites for the financial transactions like online banking.

Figure 7: Blank Keyboard with Special Symbols

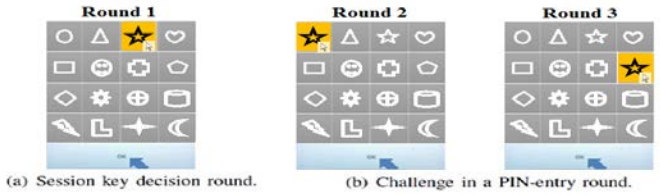

Figure 8: Example of a session key decision procedure and a PIN-entry procedure for PIN 2371, in which the session key is given as O.

In the example shown in (a), where the PIN is 2371, the user recognizes as the session key because it is collocated with the first digit of the PIN, 2. The remaining rounds are PIN-entry rounds, in which the ith digit of the PIN is entered in the ith round for i = 2; 3; 4. In each of these rounds, the user is again given a random array of 16 objects as in (b), and s/he enters a PIN digit by dragging and changing the object array and aligning the session key with the current PIN digit, as in (c). This input mechanism can be implemented using various devices, such as keypads, touchscreens.

4. CONCLUSION:

In this paper, a new authentication method to enter the credentials to the online sites to perform transactions or in ATM to enter the PIN is proposed. This method is a quantitative security notion for PIN-entry methods, and a novel theoretical and experimental technique to analyze security. This new method is resistant against most powerful attacks – key logging and shoulder surfing attacks. This was possible by increasing the amount of memory required by a shoulder surfer and using a blank keyboard layout. This method will be user friendly. But for some special users like elder persons, it may be difficult to perform these much operations. So we can incorporate this method into any sites for doing financial transactions by keeping the existing method of entering the passwords through keyboard or virtual keyboard. We can switch between these methods by making a selection. Also, these attacks are more prominent if we perform the transactions from a public place or public computer. If we are using from our personal system from our home, there is only less chance of attacks. So switching between these two methods will be more useful. This method is not suitable to be used in places where recording can be done without raising suspicion, e.g., a store with a surveillance camera.

5. REFERENCES:

1. D. Nyang, A. Mohaisen and J. Kang, “Keylogging-resistant Visual Authentication Protocols,” in IEEE Transactions on Mobile Computing, 2014, pp.1-14.
2. Mun-Kyu Lee, “Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry,” in IEEE Transactions on Information Forensics and Security, 2014, pp. 695 – 708.

3. Bin B. Zhu, Dongchen Wei, Maowei Yang and Jeff Yan, "Security implications of password discretization for click-based graphical passwords," in WWW '13 Proceedings of the 22nd international conference on World Wide Web, ACM 2013, pp. 1581-1591.
4. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in ESORICS, 2008.
5. Alain Forget, Sonia Chiasson and Robert Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords" in CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM 2010, pp. 1107-1110.
6. M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder surfing by using gaze-based password entry," in ACM SOUPS, 2007, pp.13–19.
7. J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in IEEE Symposium on Security and Privacy, 2005, pp.110–124.
8. C. S. Kim and M.-K. Lee, "Secure and user friendly PIN entry method," in 28th International Conference on Consumer Electronics (ICCE 2010), IEEE, 2010, pp. 203- 204.
9. C. Topal, B. Benligiray and C. Akinlar, "On the efficiency issues of virtual keyboard design," in IEEE International Conference on Virtual Environments Human-Computer Interfaces and Measurement Systems (VECIMS), 2012, pp. 38- 42.
10. Ankit Parekh, Ajinkya Pawar, Pratik Munot and Piyush Mantri, "Secure Authentication using Anti-Screenshot Virtual Keyboard," in International Journal of Computer Science Issues(IJCSI), Vol. 8, 2011.
11. Yang Xiao; Chung-Chih Li; Ming Lei; Vrbsky, S.V., "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password Theft," Systems Journal, IEEE , vol.8, no.2, pp.406,416, June 2014.