International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Sophisticated Approach to Graphical Password

Ansiya A[1], L M Bernald[2]

[1]*PG scholar, Dept.Of Computer Science Engineering, Rajadhani Institute of Engineering and Technology, Kerala, India*
[2]*HOD, Dept.Of Computer Science Engineering, Rajadhani Institute of Engineering and Technology, Kerala, India*

Abstract-*This evolution brings great convenience to secure computer world. Attackers can observe directly or use external recording devices to collect users' credentials like passwords/pin numbers. To overcome this problem, we proposed a novel authentication system based on graphical passwords named passmatrix, to resist shoulder surfing attacks even they conduct multiple camera-based attacks. With a one-time valid login indicator comprised of a letter and a number and circulative horizontal and vertical bars covering the entire scope of pass images, PassMatrix offers no hint for attackers to figure out or narrow down the password. From the study, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.*

Key Words: **Graphical Passwords, Authentication, Shoulder Surfing Attack.**

1. INTRODUCTION

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect [1]. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts [2]. There are numerous graphical password authentication schemes [3], [4], [5] exist and weaknesses associated with textual passwords. Image-based passwords were proved to be easier to recollect in several user studies.

Users can set up a complex authentication password and are capable of reentering it after a long time even if the memory is not use periodically. However, most of these image-based passwords not secure because of shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone or applies video capturing techniques to get passwords, PINs, or other personal information .All human actions such as choosing bad passwords or inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication mechanism [8]. An authentication scheme which is designed to overcome these vulnerabilities named PassMatrix that protects users from becoming victims of peeping attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated number or text for each pass-image .after session terminates it will disappear. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to fix the position of their passwords.

1.1 Assumptions

In graphical password do not discuss the movements and the preference of users that the attacker may take advantage of to figure out the potential passwords. In addition, we have four assumptions in this study:

1) Any communication between the client device and the server is protected by SSL so that information will not be intercepted by attackers during transmission.

2) The server and the client devices in our authentication system are protected.

3) The keyboard and the entire screen of mobile devices are difficult to protect, but a small area (around 1:5 cm2) is easy to be protected from malicious people who might copy the passwords.

4) Users are able to register an account in a place that is safe from attackers or surveillance cameras that are not under proper management

2. LITERATURE REVIEW

2.1The Design and Analysis of Graphical Passwords

In 1999, Jermyn et al. proposed Draw-a-Secret (DAS) [4] technique where the user is required to re-draw a predefined picture on a 2D grid. This paper had proposed and evaluated new graphical password to achieve better security than text based passwords. Graphical input devices enable the user to eliminate the position of inputs from the temporal order in which those inputs occur, this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of schemes, it devised a way to capture a subset of the memorable passwords. This paper had explored an approach to user authentication that conclude the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. It designed and analyzed graphical passwords, which can be input by the user to any device with a graphical input interface. A graphical password serves the same result as a textual password, but can consist,

the devices are personal digital assistants" (PDAs) such as the PalmPilotTM, Apple NewtonTM, Casio Cassiopeia E-10TMw a pre-defined picture on a 2D grid. However, this authentication schemes are still vulnerable to attacks as they may reveal the graphical passwords directly to some unknown observers in public.

2.2 Pass Points: Design and longitudinal evaluation of a graphical password system

In 2005, Susan Wiedenbeck et al.introduced a graphical authentication scheme Passpoints [5], a new and secure graphical password, which consists of clicking on images better than typing alphanumeric strings, may help to overcome the problem of creating secure passwords. We report a study comparing the use of PassPoints to alphanumeric passwords. Participants created an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password. The results show that the graphical password users created a valid password with difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords. In the trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password. This authentication scheme is still vulnerable to attacks

2.3 A Pin Entry Method Resilient Against Shoulder Surfing

In 2004, Roth et al. [9] presented an approach for PIN entry against shoulder surfing attacks by increasing the noise to observers. In their approach, the PIN digits are displayed in either black or white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system configure out the PIN number the user intended to enter by intersecting the user's choices. Towards a PIN entry method that is robust against shoulder surfing, proposed two variants of an interactive challenge-response protocol to which we refer as cognitive trapdoor games. The essential feature of such a game is that it is easily won if the PIN is known, and hard to win otherwise. The cognitive capabilities of a human are generally not sufficient to derive the genuine PIN through observation of the entire game's input and output. This approach could confuse the observers if they just watch the screen without any help of video capturing devices. However, if observers are able to capture the whole authentication process, the passwords can be cracked easily.

2.4 fakePointer: An Authentication Scheme for a Better Security against a Peeping Attack by a Video Camera

In order to defend the shoulder surfing attacks with video capturing, FakePointer [7] was introduced in 2008 by T. Takada. In addition to the PIN number, the user get a new "answer indicator" each time for the authentication process at a bank ATM. At each login session, the FakePointer interface will present the user an image of a numeric keypad with 10 numbers (similar to the numeric keypad for phones), with each key (number) on top of a randomly picked shape. The numeric keys, but not the shapes, can be moved circularly using the left or right arrow keys. During authentication, the user must repeatedly move numeric keys circularly, until the first digit of the PIN overlaps the first shape of the answer indicator on the keypad and then confirm a selection by pressing the space key. This operation is repeated until all the PIN digits are entered and confirmed. This approach is quite difficult even when the attacker captures the whole authentication process. However, there is still room to improve the password space. For example, if the device used for authentication is a smartphone, a tablet or a computer rather than a bank ATM, the password space can be enlarged substantially since the PIN could be any combination of alphanumeric characters rather than just numeric digits.

2.5 Multi-Touch Authentication on Tabletops

In 2010, David Kim et al. [8] proposed a visual authentication scheme for tabletop interfaces called "Color Rings" [9]),where the user is assigned i authentication (key) icons, which are collectively assigned one of the four color-rings red, green, blue, or pink. During login, i grids of icons are provided, with 72 icons being displayed per grid. There is only one key icon presented in each grid. The user must drag all four rings (ideally with index finger and thumb from two hands) concurrently and place them in the grid. The distinct key icon should be captured by the correct coloring while the rest of rings just make decoy selections. The user confirms a selection by dropping the rings in position. The rings are large enough to include more than one icon and can thus obfuscate the direct observer. Unfortunately, these kinds of passwords can be cracked by intersecting the user's selections in each login because the color of the assigned ring is fixed and a ring can include at most seven icons. Thus, the attacker only requires a limited number of trials to guess the user's password.

3. PROBLEM DEFINITION

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account anytime and anywhere. While logging into these services in public, they may expose their passwords to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window. Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to one's assets the following

lists the research problems we would like to address in this study:

1) The problem of how to perform authentication in public so that shoulder surfing attacks can be alleviated.

2) The problem of how to increase password space than that of the traditional PIN.

3) The problem of how to efficiently search exact password objects during the authentication phase.

4) The problem of requiring users to memorize extra information or to perform extra computation during authentication.

5) The problem of limited usability of authentication schemes that can be applied to some devices only.

4. ATTACK MODEL

4.1 Shoulder Surfing Attacks

Based on previous research [9], users 'actions such as typing from their keyboard or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. In this paper, based on the means the attackers use, we categorize shoulder surfing attacks into three types as below:

1) Type-I: Naked eyes.

2) Type-II: Video captures the entire authentication process only once.

3) Type-III: Video captures the entire authentication process more than once.

The latter types of attacks require more effort and techniques from attackers. Thus, if an authentication scheme is able to resist against these attacks, it is also secure against previous types of attacks. Some of the proposed authentication schemes [4], [5], [6], [7], including traditional text-password and PIN, are vulnerable to shoulder surfing Type-I attacks and thus are also subject to Type-II and Type-III attacks. These schemes reveal passwords to attackers as soon as users enter their passwords by directly pressing or clicking on specific items on the screen. Other schemes such as those in can resist against Type-I but are vulnerable to Type-II and Type-III attacks since the attackers can crack passwords by intersecting their video captures From multiple steps of the entire authentication process.

3.1 Smudge Attack

According to a previous study that require users to touch or fling on computer monitors or display screens during the login phase are vulnerable to smudge attacks. The attacker can obtain the user's password easily by observing the smudge left on the touch screen

Fig-1: The residue from fingerprints

5. METHODOLOGY

5.1 Passmatrix

To overcome

(1) The security weakness of the traditional PIN method

(2) The easiness of obtaining passwords by observers in public

(3) The compatibility issues to devices

Introducing a graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one pass-square for each pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints [5] scheme. Based on the user study of Cued Click Points (CCP) proposed by Chiasson et al

Fig-2: password contains three images (n=3) with a pass square in each. The pass squares are shown as the orange-filled area in each image.

The CCP method does a good job in helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image, a different image will be shown to give the user a warning feedback. However, aiming at alleviating shoulder surfing attacks Due to the fact that people do not register a new account or set up a new screen lock frequently, we assume that these setup events can be done in a safe environment rather than in public places. Thus, users can pick up pass-squares by simply touching at or clicking on them during the registration phase.

1. Registration phase

The user creates an account which consists of username and a password. The password contains only one pass-square per image for a sequence of n images. The number of images is decided by the user. The only purpose of the username is to give the user a personal account. The username can be omitted if PassMatrix is applied to authentication systems. The user can either choose images from a provided list or upload images from their device. Then the user will pick a passsquare for each selected pass-image from the grid view, which was divided by the image. The user repeats this step until the password is set.

2 Authentication phase

The user uses username, password and login indicators to log into PassMatrix. The following describes all the steps in detail:

1) The user inputs username which was created in the registration phase.

2) A new indicator comprised of a letter and a number is created by the login indicator generator module.. The indicator can be delivered to user by email.

3) Next, the first pass-image will be shown on the display, consist of horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user drags the bars to align the pre-selected pass-square of the image with the login indicator.

4) Repeat step2 and step 3 for each pre- selected passimage.

5) The communication module gets user account information from the server through HttpRequest POST method.

6) Finally, for each image, the password verification module verifies the correctness between the passsquare and the login indicator. Only if all the details are correct in all images, the user is allowed to log into PassMatrix

6. IMPLEMENTATION

In the client side of our prototype, we use XML to build the user interface and used JAVA to implement functions, including username verification, listing of passimage image discretization, selection of pass-squares, login indicator delivery, and scrolling of horizontal and vertical bars. In the server side of our implementation, we used java and MySQL to store and fetch registered accounts to/from the database to handle the password verification.

7. PRELIMINARY DATA

As the mobile marketing statistics compilation by Danyl, the mobile shipments had overtaken PC shipments in 2011, and the number of mobile users also overtaken desktop users at 2014, which closed to 2 billion. However, shoulder surfing attacks have posed a great threat to users' privacy and confidentiality as mobile devices are becoming essential thing in modern life. People may log into web services and apps in public to access their personal accounts with their smart phones, tablets or public devices, like bank ATM. Shoulder-surfing attackers can observe how the passwords were entered with the help of reflecting glass windows, or alone monitors hanging everywhere in public places. Passwords are exposed to risky environments, even if the passwords themselves are complex and secure. A secure authentication system need to be able to defend against shoulder surfing attacks and should be applicable to all kinds of devices. Authentication schemes in the literature such as those in [6] are resistant to shoulder-surfing, but they have either usability limitations or small password space. The limitations of usability include issues such as taking more time to log in, passwords being too difficult to recall after a period of time, and the authentication method being too complicated for users without proper education and practice. In 2006, Wiedenbeck et al. proposed PassPoints [5] in which the user picks up several points (3 to 5) in an image during the password creation phase and re-enters each of these pre-selected click-points in a correct order within its tolerant square during the login phase. Comparing to traditional PIN and textual passwords, the Pass- Points scheme substantially increases the password space and enhances password memorability. Unfortunately, this method of graphical authentication scheme is vulnerable to shoulder surfing attacks. Hence, based on the PassPoints, we implement the idea of using one-time session passwords and PassMatrix authentication system that is resistant to shoulder surfing attacks.

7. LIMITATIONS

It can not be applicable to small scale systems such as simple user application like social network, email, online shopping etc…

- It is time consuming
- User need to login their email to perform login

8. CONCLUSION

We present a secure graphical authentication system that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of the one-time login indicators. The login indicator is randomly generated for pass-images and will be useless

after the session terminates. The login indicator provides better security against attacks, since users use a dynamic selection to figure out the location of their passwords rather than clicking on the password object directly. Based on the experimental results and survey data, PassMatrix is a novel and easy-to-use graphical password authentication system, which can effectively solve the shoulder-surfing attacks. The survey data in the user study also showed that PassMatrix deployment is practical in the real world.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479–483.

[3] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[4] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1, 2005

[5] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies,vol. 63, no. 1-2, pp. 102–127, 2005.

[6] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect,"Journal of Experimental Psychology: Human Learning and Memory,vol. 3, pp. 485–497, 1977.

[7] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trasactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6,pp. 716–727, June 2014.

[7] T. Takada, "fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM' 08. The Second International Conference on. IEEE, 2008, pp.395–400.

[8] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.

[9] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACMconference on Computer and communications security, ser. CCS '04.New York, NY, USA: ACM, 2004, pp. 236–245.