

**Multi-Approached Graphics Based Authentication**Akshay Kshirsagar¹, Manmath Markunde², Umesh Patil³^{1,2,3}Department of Computer Engineering, Dr. D. Y. Patil College of Engineering, Ambi

Abstract — Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session. When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. There have been some graphical schemes resistant to shoulder-surfing, but they have significant usability drawbacks, usually in the time and effort to log in. In this paper, we propose a password scheme. This is obtained by adding a little Graphic Layer to the Traditional Text based Password Scheme. In This Layer We Randomly Generate Patterns of icons which are easy for a user who owns the password to recognize and difficult for a shoulder surfing attacker to find out. Pass Matrix Algorithm is used for Pattern Generation. It is defined as challenge-response identification. Hence, a password in our scheme is time-variant. User who knows the password is able to meet the challenge and to respond correctly. As a consequence, our graphical password scheme is shoulder-surfing resistant. An attacker still cannot tell what the password is, even if he/she has involved in user login process.

Keywords - Graphical Passwords, Authentication, Shoulder Surfing Attack.

I. INTRODUCTION

Current authentication systems suffer from many weaknesses. The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords unprotected for attackers to break. Furthermore, textual password is vulnerable to guessing, dictionary attack, key loggers, and social engineering, shoulder surfing, hidden-camera and spyware attacks. To conquer the limitations of text-based password, techniques such as two-factor authentication and graphical password have been put in use. Other than that, applications and input devices such as mouse, stylus and touch-screen that permit make the appearance of the graphical user authentication techniques possible. However, they are mostly vulnerable to shoulder-surfing as well.

Passwords possess many useful properties as well as widespread legacy deployment; consequently we can expect their use for the foreseeable future. Unfortunately, today's standard methods for password input are subject to a variety of attacks based on observation, from casual eavesdropping (shoulder surfing), to more exotic methods. Shoulder-surfing attack occurs when using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information. As well as when a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. This is a problem that has been difficult to overcome.

Now a days computer as well as information security is the most significant challenge. Authorized users should access the system or information. Authorization cant occur without authentication. For this authentication various techniques are available. Among them the most popular and easy is the password technique. Password ensures that computer or information can be accessed by those who have been granted right to view or access them. Traditional password technique is a textual password which is also called alphanumeric password. But these textual passwords are easy to crack through various types of attack. So to overcome these vulnerabilities, a graphical password technique is introduced. As name suggests in this technique images (pictures) are used as a password instead of text. Also psychological study says that human can easily remember images than text. So according to this fact, graphical passwords are easy to remember and difficult to guess. But because of graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack. So here, a new graphical password authentication technique is proposed which is resistant to shoulder surfing and also other types of possible attacks to some extent.

II. LITERATURE SURVEY**1. Reducing Shoulder-surfing by Using Gaze-based Password Entry**

Authors: Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd

Description:

The Shoulder-surfing – is using direct observation techniques, such as looking over someone's shoulder, to get passwords credentials, PINs and other sensitive personal information – is a issue that has been difficult to overcome. When a user enters information using a keyboard, mouse or any traditional input device systems, a malicious user may be able to acquire the user's password credentials. We introduced EyePassword, a system that mitigates the problems of shoulder surfing attack via a novel technique to user input. With EyePassword, a user enters sensitive input such as password, PIN,

etc. by choosing from an on-screen keyboard using only the orientation of their eye pupils i.e. the position of their gaze on screen, making eavesdropping by a malicious person largely impractical. We introduce a number of design choices and discuss their effect on usability and security. We conducted user studies to evaluate the speed, accuracy and user acceptance of our methodology. The results shows that gaze-based password entry requires marginal additional time over using the keyboard, error rates are same as to those of using a keyboard and subjects preferred for the gaze-based password entry techniques over traditional methods.

2. Graphical Password Authentication

Authors: ShraddhaM. Gurav Leena S. Gawade Prathamey K. Rane, Nilesh R. Khochare

Description:

Graphical password is the one of the best alternative solution to alphanumeric password as it is very tedious procedure to remember of alphanumeric password. When any application is provided with user friendly authentication it becomes simple to access and use that application. One of the major reasons behind this approach according to psychological studies that human mind can easily remember the images than alphabets or digits. In this paper we are introducing the authentication given to cloud by using graphical based password. We have presented the cloud with graphical security by means of image password. We are providing one of the algorithmic approaches which are based on selection of username and images as a password. From this paper authors are planning to give set of images on the basis of alphabet sequence position of characters in username. Finally cloud is provided with this graphical password authentication.

3. S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme

Authors: Huanyu Zhao and Xiaolin Li

Description:

The difficulties of the textual password have been well known to us. Users tend to pick small passwords or passwords that are simple to remember to mind, that makes the passwords vulnerable for malicious user to break. Furthermore, textual based password is vulnerable to shoulder-surfing, hidden camera. Graphical based password approaches have been introduced as a possible solution to text-based scheme. However, they are mostly vulnerable to shoulder surfing attacks. In this paper, presented a Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS). The S3PAS seamlessly combines both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing, hidden-camera attacks. It can replace or overcome with conventional textual based password schemes without changing current user password profiles. Moreover, it is immune to the brute-force attacks through dynamic and volatile the session passwords. The S3PAS shows significant potential bridging the gap between conventional textual based password and graphical based password.

4. D'ej`a Vu: A User Study Using Images for Authentication

Authors: Rachna Dhamija Adrian Perrig

Description: Present secure systems suffer because they neglect the importance of human factors in security. We address a fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember the secure passwords. Our methodology to improve the security of these systems relies on recognition-based, rather than recall-based authentication. We examine the requirements of a recognition-based authentication system and propose D'ej`a Vu, which authenticates a user through her ability to recognize previously seen images. D'ej`a Vu is more reliable and easier to utilize than traditional recall-based schemes, that requires the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others.

5. PassPoints: Design and longitudinal evaluation of a graphical password system

Authors: Susan Wiedenbecka,_, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memon

Description:

The Computer security depends mostly on the passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is huge and random. Therefore, they tend to select short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to resolve the issue of creating the secure and memorable passwords. In this paper we describe PassPoints, a new and more secure graphical password system. We report an empirical study comparing the use of PassPoints to the alphanumeric passwords. The users created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to the input their password over the duration of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took long lengthy and made much invalid password inputs than the

alphanumeric users while practicing their passwords. In the longitudinal trials the two different clusters performed similarly on memory of their password, but the graphical group appears more time to input a password.

III. PROPOSED SYSTEM

The Passwords remain the dominant means of authentication in day today's systems due to of their simplicity, legacy deployment and ease of revocation. Unfortunately, common approaches to entering passwords by the way of keyboard, mouse, touch screen or any traditional input device, are mostly vulnerable to attacks such as shoulder surfing attack and password snooping attack. Present approaches to reducing shoulder surfing typically also decrease the usability of the system; mostly requiring users to use security tokens, interact with systems that do not provide direct feedback or they need additional phases to prevent an malicious observer from easily disambiguating the input to determine the password/PIN. Previous gaze-based authentication methods do not support traditional password schemes.

We present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

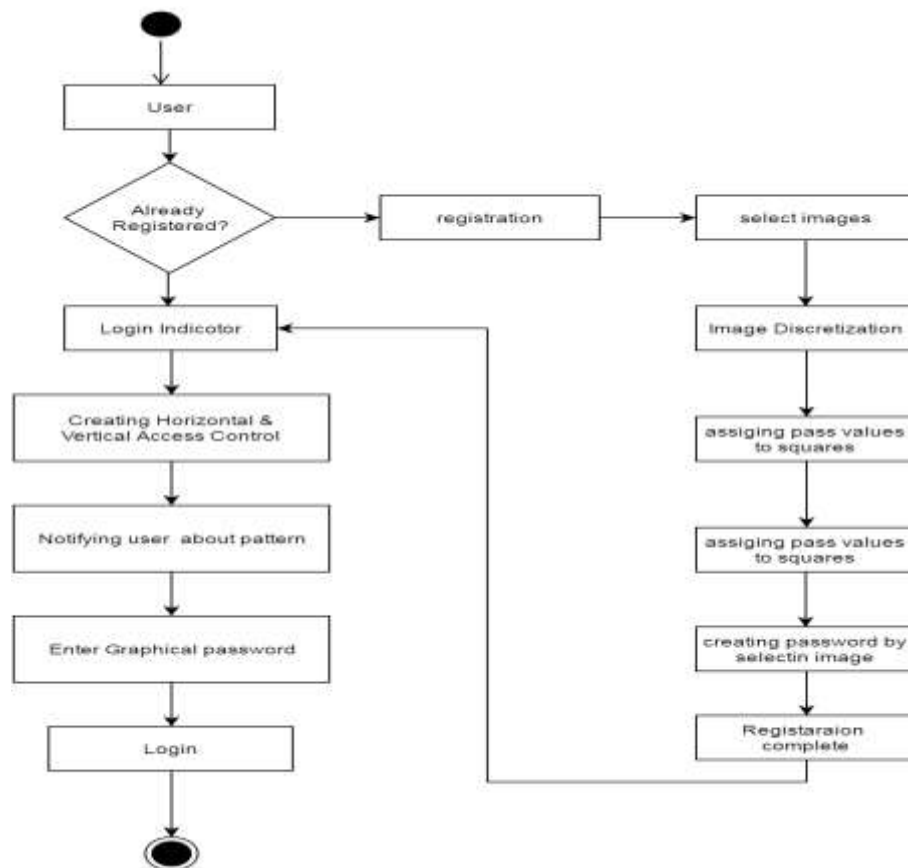


Fig.1 Activity Diagram

IV. MODULES

1. Image Discretization Module. This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 5, an image is divided into a 7×11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations on palm-sized mobile devices.

2. Login Indicator Generator Module. This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In our implementation, we used characters A to G and 1 to 11 for a 7×11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called. The generated login indicator can be given to users visually or acoustically in our system we are sending this patterns on users email.

3. Horizontal and Vertical Axis Control Module. There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers.

4. Communication Module. This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

5. Password Verification Module. This module verifies the user password during the authentication phase. A pass Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green). square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

V. METHODOLOG OF PROPOSED SYSTEM

1. Registration phase

The user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a pass square for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

2 Authentication phase

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

- 1) The user inputs his/her 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 will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can be delivered to user by email.
- 3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is (E, 11) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character "E" to the 5th column on the horizontal bar and "11" to the 7th row on the vertical bar
- 4) Repeat step 2 and step 3 for each pre-selected pass image.
- 5) The communication module gets user account information from the server through Http Request POST method.
- 6) Finally, for each image, the password verification module verifies the alignment between the passquare and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

VI. SUMMERY AND CONCLUSION

Introduced a shoulder surfing attack resistant authentication system on graphical based passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square values without directly clicking it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. Furthermore, we implemented a PassMatrix prototype on web based application and carried out user experiments to evaluate the memorability and usability the system. Based on the analytical results and survey data, PassMatrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks. In addition, PassMatrix can be applied to any authentication scenario and device with simple input and output capabilities. The survey data in the user study also showed that PassMatrix is practical in the real world.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributors for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

- [1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transactions on Dependable and Secure Computing, 2016.
- [2] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.
- [3] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467–472.
- [4] 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.
- [5] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.
- [6] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005. 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.
- [7] 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.
- [8] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.
- [9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.
- [10] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, "Vip: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.