Graphical Password Authentication Using Partioning A Secret

Ankit Gupta[1], Sanjay Gupta[2]
[1]Dept of CSE
[2]Assistant Professor, Dept of CSE
[1, 2] Vindhya Institute of Technology & Sciences, Jabalpur, Madhya Pradesh, India.

Abstract*- Internet services such as social networks, e-banking, email, cloud services, blogs, all require some form of security like user authentication. Despite the availability of advanced authentication technologies such as smart cards, biometrics or USB tokens, passwords and PINs are still the most prevalent form of user authentication. Graphical passwords are a form of user authentication on which a lot of research has been undertaken over the past decade and a variety of alternative password schemes proposed. Proposed system develops image based and portioning based authentication method. It provides user to select image and grid pattern for making partition password. It was found that brute-force attacks were largely ineffectual in terms of time required although image analysis had a profound impact on the effective password space. Password generated by this algorithm is more memorable than pass point mechanism. Proposed system is user friendly, effective, efficient, multifactor and multilayer authentication system. It keeps resistance against information leaks, brute force attack, phishing attacks, replay attack and man-in-the-middle attack*

Keywords*-* Security, Authentication, Multifactor authentication, Graphical Password, Image Pattern, PAS.

I. INTRODUCTION

The convenience of smart phones coupled with its increasing functions (e.g., provided by various APPs) has enabled users to collect and store various kinds of data, much of which are highly personal or sensitive such as photos, emails, phone call logs, chat messages, location traces or even confidential business documents, and access them at anytime and anywhere. As they are carried nearly everywhere we go, smart phones are also prone to be lost or stolen, or subject to unwanted access. Securing mobile devices such as smart phones against unauthorized access is therefore critical in protecting user's personal data and privacy. The most common authentication approach for smart phones is to use a PIN or pattern lock when reactivating the screen. With more resources (i.e. information and services) are going online, the need for control protection for users to access such resources are critical. It is anticipated that one of many steps to achieve such protection are known as authentication and authorization. Generally, user authentication can be explained as a process of proving who the user is to the resources. As time goes on, studies have revealed that using long and complex combinations of password can cause problems with ease of use and memorability, and using simple passwords resulted in a range of security problems. As the consequences, alternative technologies such as the use of token, biometric, cognitive passwords as well as using sign-on and public key cryptography are gaining much attention to replace and overcoming problems in the password-based authentication. It is anticipated that each of these technologies has their own weaknesses and strengths. Thus, observation was made to identify potential alternatives for password-based authentication, by which the use of images (known as 'graphical passwords') was found.

1.1 Overview of authentication:

Many network security researches imply a key area called as authentication that gives a response from checking whether the user should be allowed to access a given system or resource, to protect underlying networking infrastructure from unauthorized access, malfunction, destruction, misuse or improper disclosure, so that a secure platform for computers, users and programs to perform, is created. The objective of Internet security is to establish rules and measures to use against attacks over the Internet. The usage of Internet has drastically expanded over the years. People use Internet to transfer confidential information. Security is needed to prevent unauthorized use of such information. Therefore the need for security has become indispensible in this era. A network needs security against attackers and hackers. Figure below shows the authentication process.

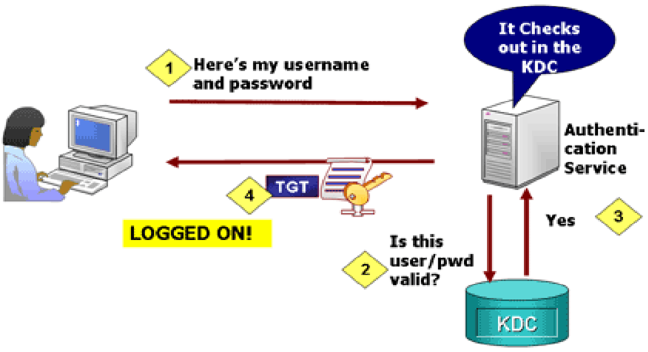

Figure 1.1: Overview of authentication.

Network Security includes two basic securities: first is the security of data information and the second is computer security (i.e.) to protect data and to thwart hackers. The unauthorized access of information led to unfortunate consequences to the victim. The passwords used initially were text passwords. These passwords were composed of logical set of characters relating to the user. This enables text password offenders to gain access to confidential information of people through various prevailing attacks. Text passwords were the pioneer in the field of security. These were easy to remember. However, these passwords were more prone to attacks as they were easy to guess. A password manager stores the text passwords for the websites hosting user accounts and sends the passwords to the user when they are required. The issue behind the text passwords is that an attacker can access the master password which provides control to the user managed accounts [1]. CAPTCHA is a password system that cannot be solved by computer programs or bots, but the human can solve [2]. CAPTCHA differentiates genuine users and automated scripts developed by attacks [3]. CAPTCHA can be classified into three text-based CAPTCHA, image-based CAPTCHA and video/audio based CAPTCHA. The Text-based CAPTCHA allows the users to decipher text that is in the form of an image. For example, GIMPY CAPTCHA, EZGIMPY CAPTCHA, AltaVista CAPTCHA, ScatterType CAPTCHA, Mega upload CAPTCHA, MSN CAPTCHA. In the case of image-based CAPTCHA, the passwords are displayed as images (i.e.) the user selects the images as an entry to passwords. For example, ESP-PIX, KittenAuth, Asirra. These CAPTCHAs lay bare a flaw is that random guessing's solutions can have a high probability of success. To overcome this problem, Scene Tagging CAPTCHA, MosaHIP, IMAGINATION CAPTCHA is used as image-based CAPTCHAs. Video-based CAPTCHA functions by posturing tagged videos with graphic text. (e.g.) Kluever. Audio-based CAPTCHA is mainly prepared for visually-impaired users by recording the texts which they are asked to enter [4].

Graphical password is a knowledge based authentication mechanism where the user enters a shared secret as evidence of the user's identity. The user is required to remember an image as password instead of a word with characters and numbers. There are three types of graphical passwords: click-based graphical passwords, (recall-based graphical passwords) cued-recall graphical passwords and recognition based graphical passwords. The graphical passwords improve password memorability and strength against guessing attacks. The graphical passwords are multi-fold, so that the usage of the graphical passwords is expanded from sign in to a personal computer, to a large number of distributed systems hosting individual information and commercial or business information and to authorize e-payable transactions via wireless devices.

PassPoints (hot-spots) are a type of graphical passwords. This allows the user to select a series of points on a displayed image [5]. Graphical coordinates of selected points are given directly to the authentication server for authentication process. There are three kinds of click-order patterns used: DIAG, LINE and Localized Omni-Direction. DIAG includes a sequence of click-points with vertical and horizontal direction. LINE includes a sequence of click-points with either a vertical direction or a horizontal direction. Localized Omni-Direction includes a sequence of click-points in which two consecutive points are constrained by a predefined distance constraint. Spyware is software that collects details of the computer's usage and transmits the information back to an unauthorized person. The spyware attack is observed by an automated program called CAPTCHA [6]. Online password guessing attacks are most commonly viewed against web based applications and Secured SHell logins [7]. These attacks include brute-force attacks and online dictionary attacks. Relay attack can be distinguished as man-in-the-middle attacks and replay attacks. In relay attack, a fake attacker intercepts and manipulates the information and relays that message between a valid sender and a valid receiver. Shoulder-surfing attack occurs when an individual is eavesdropping over person's shoulder to obtain passwords, PINs and secured personal information.

1.2 Smartphone authentication using multitouch:

Now a days, multi-touch phones and tablets have grown rapidly. More than 60 million mobile devices in the world use multi-touch capabilities. This multi-touch interfaces bring new capabilities to existing devices and enable their use in completely new contexts. Now this technology currently viewed in multi-touch devices such as smart phones, tablets, coffee tables in our living rooms, and desks in our offices. It is an attractive user interaction features and the visual experience provided by multi-touch interfaces, make them strong contenders for becoming the dominant human computer interface, possibly replacing the keyboard, mouse and stylus. The biometrics refers to the automatic identification of human beings based on their physical or behavioral characteristics. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour / scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

1.3 Multi-touch gesture based authentication

In a biometric authentication system, the identity of the user is given to the system along with a proof of identity. Correctness of the proof of identity is then evaluated by the system. After that, the answer, either accepts or rejects the user, is given based on the evaluation result. In order to verify the proof, the system needs to have a prior knowledge about it. To achieve this, there are generally two stages in a verification system: enrollment stage and verification stage. The purpose of the enrollment stage is to register the user's data in the system by acquiring and storing biometric templates corresponding to the user. In the verification stage, the input biometric instance is compared with the stored biometric templates of the claimed identity in order to authenticate a user. The term "graphical password" refers to a user authentication method where pictorial information is used for validation, instead of an alphanumerical password. This method poses many challenges, such as memorability (which refers to how easy the password is to remember), usability, and security, since graphical passwords may tend to be visually simple and easily forged.

II. LITERATURE SURVEY

Authentication is classified as a one-to-one process that enables a device or system to verify or identify someone's identity. The process usually requires a person to assert some claims which are used to determine if a person is who they claim to be. Authentication is widespread in many environments, especially work environments that protect critical resources, such as user information. A common problem related to authentication is the cost, as well as the type of authentication, as opposed to the resources protected. The specific claims are determined by the type of authenticator [8]. These authenticators can be distinguished as follows:

- *Something the user knows:* Typically passwords, passphrases, associations or PIN.
- *Something the user possesses:* Token such as smartcards, magnetic cards typically used in conjunction with something the user knows.
- *Something the user is:* Biometric systems, based on the unique physiological, psychological or behavioral human traits.

This chapter gives details of different Graphical Password generation techniques implemented. Along with it, we have the previous and yet emerging algorithm in support that provides guidelines in investigation and pursuit of our advanced proposed scheme. We hereby, describe the study performed prior to developing the proposed system.

The tremendous advancement in technology over the past decades made internet an efficient and universal platform for various services ranging from financial transactions to simple email access. Apparently, this advancement also gave rise to security threats, thereby making information security as the promising area of concern. Authentication is the basic component in this security context, and is defined as the process of confirming user's claimed identity.

This is primarily due to simplicity and low cost of their creation, maintenance and revocation. The computer system today that requires its users to authenticate themselves uses the traditional authentication scheme that has the user enter a secret of their choosing, i.e. a password. Once a password has been entered, the system looks up the entered username and password in the password hash [9]. If the system's stored password matches the entered password for the specified username, the user is authenticated with that system. This is called a Password Authentication (PA) scheme. In general, information sharing applications rely on variety of identifiers that combined, allow the application to authenticate and authorize access to the data. Several secure password selection approaches that take into account usability, have been proposed but the mechanisms are mostly complex and result in users developing alternative coping behaviours that lead to insecure systems. For instance, users typically use the same "easy-to-remember" password across different web applications because of the difficulties the users face in recalling the password and the wait-time typically required to receive permission to reset the password [10, 11].

Studies have shown that graphical passwords are a better alternative to text-based passwords from the memorability and usability perspective [12]. Furthermore, psychologists have shown, with both recognition and recall tasks, that image are more memorable to humans than words or sentences [13]. Both these arguments make graphical passwords a good alternative to consider over text-based passwords with respect to authentication mechanisms for information sharing applications. To address this issue, we present a new point-click and image-part ion graphical password system that increases resistance to observation attack by coupling the user's password to an image or object physically possessed.

2.1 Types of Authentication

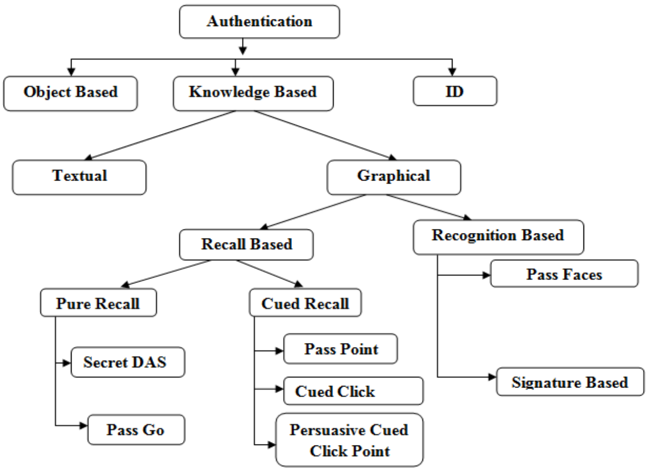

Figure 2.1 Authentication Types.

Authentication is defined as the process which positively verifies the user identity, device, or other entity in a computer system, in order to allow access to resources in the system.

2.2. Image Based Authentication

The Image-based authentication is based on Recognition Techniques. When the user registers for first time in a web site they select set of images that are easy to remember, such as natural scenery, automobiles etc. Every time the user logs into the site, they are provided with a grid of images that is randomly generated. The user can identify the images that were previously selected by him. It is significantly easier for the user because they need to remember a few simple images only. IBA is based on a user's successful identification of his set of images. When the user logins for the first time, the website displays a grid of images, which consists of images from the user's password set mixed with other images. The user is authenticated by correctly identifying the password images. Performing brute force attacks or other attacks on such systems is very difficult. A set of different images are selected to authenticate the user. The Image Identification Set (IIS), for each user is then stored at the Authentication System. When a user logins, the IIS for that user is retrieved and used to authenticate that particular user. The system does not store the images but the categories of the images are stored in IIS as images are large files. This technique is also more secure and requires less memory. If this step is successful, next OTP is generated and send to the user email-id.

2.3 Attack Model

2.3.1 Shoulder Surfing Attacks

Based on previous research [14], 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 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 [15] 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.

III. PROPOSED SYSTEM

We propose, the graphical authentication using partitioned Images, system to provide authentication sequences that exhibit high memorability while increasing the number of possible sequences, making attack through guessing less likely to succeed. The user's authentication sequence consists of partitioned images rather than numbers but otherwise works in the same manner as a PIN system. In short, proposed system increases security by having the user not only enter one of 16 images image in proper sequence, but also to select a correct partition of the image (the partitions of each image are top, right, bottom, and left as marked by the red Xs). Users are thus selecting from 64 possible options at a time rather than ten options, like most PIN systems.

We then informally experimented with different partition sizes and users possessing different finger girths, finding that most users could reliably select images containing 4 equally-sized partitions after a brief practice session. We chose the X-shaped partition lines by appealing to the picture superiority effect: the regions could be remembered physically or by textual labels (such as top, right, left, bottom; or north, east, south, west). Furthermore, the locations of the images would be fixed (just as keyboard character locations do not change for password entry) to allow sequences to be remembered by the pictures they contained and by the location of those pictures. Note too that the picture superiority effect applies to all people: not only can the user remember images more easily than text, but so too can a malicious observer trying to steal a user's authentication sequence. Partitions help to keep proposed system resistant (but not immune) to "shoulder surfing" since an observer may be able to see what image was selected but will likely be less accurate in observing which specific partition was selected, depending on the viewing angle of the observer.

3.1 Password Creation Process

Steps for creating graphical password in proposed system are as follows:

Step-1: Select create password activity.
Step-2: Initializes resource image array with 16 images that will be shown in layout.
Step-3: Create 4X4 layout and canvas.
Step-4: Randomize all images so that every time images for cells will be different.
Step-5: Draw images into layout.
Step-6: Superimpose X shape line on every cell above images to make partition and call them field(triangular shaped). Field have unique id.
Step-7: Select any triangular field of any image and store corresponding resource image id & field id.
Step-8: Repeat step 7 six time to make a difficult, shoulder surfing free password.
Step-9: Store pasword that will be used later for authentication.
Step-10: End.

IV. IMPLEMENTATION AND EVALUATION

Evaluation of proposed system will be discussed on the basis of following issues:

- We propose the graphical password Authentication using partitioned images system to provide authentication sequences that exhibit high memorability while increasing the number of possible sequences, making attack through guessing less likely to succeed. The user's authentication sequence consists of partitioned images rather than numbers but otherwise works in the same manner as a normal system.

- Proposed method increases security by having the user not only enter one of 16 images image in proper sequence, but also to select a correct partition of the image, the partitions of each image are top, right, bottom, and left as marked by the red Xs. Users are thus selecting from 64 possible options at a time rather than ten options, like most PIN systems.

- We chose the X-shaped partition lines by appealing to the picture superiority effect: the regions could be remembered physically or by textual labels such as top, right, left, bottom; or north, east, south, west.

- In a typical password entry scenario, the user sees an on-screen dot representing each character entered in the password. This allows the user some feedback to confirm that a key was pressed, but disallows a casual observer from seeing the entered text. We adopted this approach though they also supported users entering image sequences via keyboard. Some modern mobile devices offer further feedback. For example, in password entry (not PIN entry) the Apple iTouch and iPhone devices show an enlarged version of the on-screen keyboard key each time the user taps the key in addition to showing the key character in clear text for approximately 500ms to allow the user to confirm what was entered. Given that we are trying to improve the overall security of authentication sequence entry, we decided to provide no further feedback of the image partition that was actually selected by the user.

- Partitions help to keep proposed system resistant to "shoulder surfing" since an observer may be able to see what image was selected but will likely be less accurate in observing which specific partition was selected, depending on the viewing angle of the observer. The number of successful trials for a certain number of trials is known as success rate. It is calculated as the number of trails completed without errors or restarts. Success rates are recorded for many numbers of attempts on both systems.

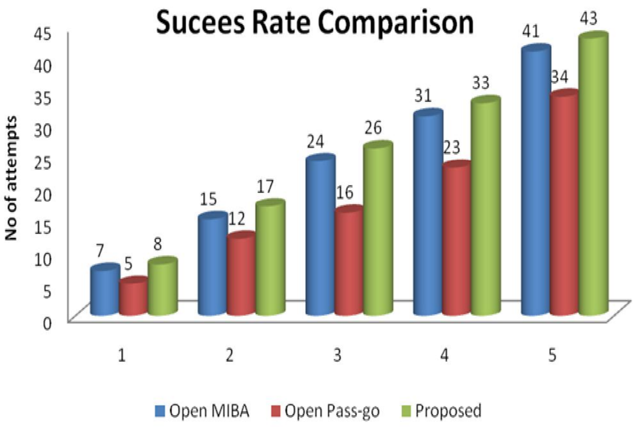

Figure 4.1: Result of success rate.

REFERENCE

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys. Vol. 44, no.4, 2012.

[2] B. B. Zhu, Jeff Yan, Qiujie Li, Chao Yang, Jia n Liu, Ning Xu, Meng Yi, Kaiwei Cai, “Attacks and design of image recognition CAPTCHAs,” in Proc. ACM CCS, 2010, pp. 187-200.

[3] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in click-based graphical passwords,” J. Comput. Security, vol. 19, no. 4, pp. 669-702, 2011.

[4] M.Motoyama, K.Levchenko, “FaceDCAPTCHA: Face Detection based color image CAPTCHA,” 2010.

[5] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on pass points style graphical passwords,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393-405, Sep. 2010.

[6] H. Gao, X. Liu, S.Wang, and R. Dai, “A new graphical password scheme against spyware by using CAPTCHA,” in Proc. Symp. Usable Privacy Security, 2009, pp. 760-767.

[7] M. Alsaleh, M. Mannan, and P. C. Van Oorschot, “Revisiting defences against large-scale online password guessing attacks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128- 141, Jan./Feb. 2012.

[8] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in *Proc. IEEE Symp. Security Privacy*, 2012, pp. 553–567.

[9] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords: Learning from the first twelve years,” *ACM Comput. Surveys* vol. 44, no. 4, p. 19, 2012.

[10] G. E. Blonder, “Graphical passwords,” U.S. Patent 5 559 961, 1996.

[11] E. Hayashi and N. Christin, “Use your illusion: Secure authentication usable anywhere,” in In Proceedings of the 4th Symposium on Usable Privacy and Security, (Pittsburgh, PA, USA, July 23-25). ACM Press, 2008, pp. 35–45.

[12] R. Biddle, S. Chiasson, and P. Van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surv. vol. 44, no. 4, pp. 19:1–19:41, Sep. 2012.

[13] Z. Zhao and G. J. Ahn, “On the security of picture gesture authentication,” in Proc. 22nd USENIX Security Symp., 2013, pp. 383–398.

[14] 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.

[15] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, “Smudge attacks on smartphone touch screens,” in USENIX 4th Workshop on Offensive Technologies, 2010.