

# Graphical Authentication System to Resist Botnet

Kirthika S<sup>1</sup> Shenbagavalli R<sup>2</sup>

<sup>1</sup>PG Student <sup>2</sup>Assistant Professor

<sup>1,2</sup>Department of Computer Science & Engineering

<sup>1,2</sup>Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India

**Abstract**— A botnet is a collection of Internet-connected user computers (bots) infected by malicious software. They can be used for many malicious purposes, including to steal user's personal data and passwords, attack public and private networks. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to botnet attacks. To make user authentication more secure by avoiding alphanumeric string which users tend to choose passwords either short or meaningful for easy memorization. To overcome this problem, we conduct a comprehensive survey of the existing graphical password techniques and proposed a new technique, proposed a novel authentication system called random pixel selection based on graphical password. Thereby, graphical authentication system called Random Pixel Selection can be done as one-time login indicator. The server would generate an image for user from the preselected images. By using Local Directional Number pattern, the features of the image are compared with generated image whether it is the user's preselected image or depredation. The proposed system achieves better resistance to Botnet attacks while maintaining usability.

**Key words:** Graphical Password, Random Pixel Selection, Local Directional Number Pattern, Security, Botnet Attack

## I. INTRODUCTION

Authenticity is the act of confirming that the truth of an attribute of a single piece of data claimed by an true entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim apparently attesting to a person or person's identity, authentication is the process of confirming that identity. It might involve to confirm the identity of a person by validating their identity documents, verifying the authenticity of a website by a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification. Textual passwords have been the most widely used authentication method for decades. Comprised of numbers, upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings which expose to botnet or shoulder surfing. A secure graphical authentication system to protect users from becoming victims of surfing attacks when inputting passwords in public through the usage of one-time login indicators. Graphical passwords are an alternative to textual alphanumeric password. It satisfies both conflicting requirements i.e. it is easy to remember and it is hard to guess.

By the solution of the botnet problem, it becomes more secure and easier password scheme.

### A. Motivation

Passwords are the most common form of authentication used to control access to information, ranging from the personal identification numbers we use for automatic teller machines, credit cards, telephone calling cards, and voice mail systems to the more complex alphanumeric passwords that protect access to files, computers, and network servers. Passwords are widely used because they are simple, inexpensive, and convenient mechanisms to use and implement. At the same time, passwords are also recognized as being an extremely poor form of protection. The Computer Emergency Response Team (CERT) estimates that about 80 percent of the security incidents reported to them are related to poorly chosen passwords. Password problems are very difficult to manage because a single local computer network may have hundreds or thousands of password-protected accounts and only one needs to be compromised to give an attacker an entry to the local system or network. With today's interconnected Internet, the problems are potentially devastating on an even larger scale; a skilful intruder may break into one system and never harm it, using it instead as a platform for attacks on a population of millions of targets [7].

The main problem with the alphanumeric passwords is that once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. If a password is not frequently used it will be even more susceptible to forgetting. The recent surveys have shown that users select short, simple passwords that are easily guessable, for example, personal names of their family members, names of pets, date of birth etc. the most important issue is having a password that can be remembered reliably and input quickly. They are unlikely to give priority to security over their need to get on with their work. Graphical password were originally described by Blonder(1996).the basic need for graphical password is that graphical passwords are expected to be easier to recall, less likely to be written down and have the potential to provide a richer symbol space than text based password. For example, a user might authenticate by clicking a series of points on an image, selecting a series of tiles, or by drawing a series of lines on the screen [11].

### B. Organization

This paper is organized as follows. Section II provides the backgrounds of related techniques about graphical authentication schemes. The proposed Random Pixel Selection is presented in Section III and Section IV concludes the paper.

## II. BACKGROUND AND RELATED WORK

In the past several decades, a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most related schemes that were mentioned in the previous section. Many other schemes such as those in [12], [13], [8], [5], [9] may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc.

In the early days, the graphical capability of handheld devices was weak; the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) [1] technique was proposed by Jermyn et al. in 1999, where the user is required to re-draw a pre-defined picture on a 2D grid. We directly extract the figure from [1] and show it in Figure 1(b). If the drawing touches the same grids in the same sequence, then the user is authenticated. Since then, the graphical capability of handheld devices has steadily and ceaselessly improved with the advances in science and technology. In 2005, Susan Wiedenbeck et al. introduced a graphical authentication scheme PassPoints [3], and at that time, handheld devices could already show high resolution color pictures. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo, as shown in Figure 1(a) (this figure is extracted from [3]), with a correct sequence and within their tolerant squares during the login stage. Moreover, Marcos et al. also extended the DAS based on finger-drawn doodles and pseudo signatures in recent mobile device [10], [11], [14], [15]. This authentication system is based on features which are extracted from the dynamics of the gesture drawing process (e.g., speed or acceleration). These features contain behavioral biometric characteristic. In other words, the attacker would have to imitate not only what the user draws, but also how the user draws it. However, these authentication schemes are still all vulnerable to shoulder surfing attacks as they may reveal the graphical passwords directly to some unknown observers in public.

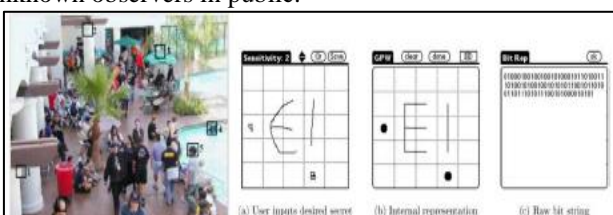


Fig. 1: (a) Pixel squares selected by users as authentication passwords in PassPoints [3]. (b) Authentication password drew by users and the raw bits recorded by the system database [1].

In addition to graphical authentication schemes, there was some research on the extension of conventional personal identification number (PIN) entry authentication systems. In 2004, Roth et al. [2] 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 can figure out the PIN number the user intended to enter by intersecting the

user's choices. However, if observers are able to capture the whole authentication process, the passwords can be cracked easily.

In order to defend the shoulder surfing attacks with video capturing, FakePointer [4] was introduced in 2008 by T. Takada. We use Figure 2 (from [4]) below to show the usage of FakePointer. In addition to the PIN number, the user will get a new "answer indicator" each time for the authentication process at a bank ATM. In other words, the user has two secrets for authentication: a PIN as a fixed secret and an answer indicator as a disposable secret. The answer indicator is a sequence of  $n$  shapes if the PIN has  $n$  digits. 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 as shown in the leftmost figure in Figure 2, 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 robust 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.

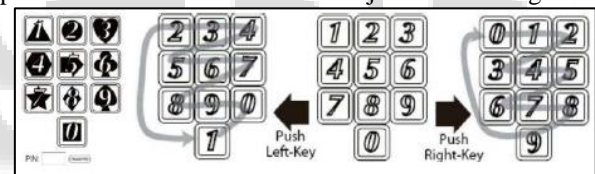


Fig. 2: FakePointer, where a user can move a numeric key layout circularly using right and left arrow keys. [4]

These techniques are developed to overcome the limitations of text-based passwords. Graphical passwords consist of recognizing the images or sometimes to recognize the image and click the particular points or area on image rather than typing the characters like text-based password. In this way, the problems that arise from the text-based passwords are reduced. Graphical password techniques were originally described by Blonder.

In 2010, David Kim et al. [6] proposed a visual authentication scheme for table-top interfaces called "Color Rings", as shown in Figure 3(a) (the figure is extracted from [6]), 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 color ring 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.



Fig. 3: (a) Color Rings method [6]. (b) Convex Hull method [6].

### III. RANDOM PIXEL SELECTION

Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies that humans have a better ability to memorize images with long-term memory than alphanumeric representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.

To overcome the security weakness of the traditional PIN method, the easiness of obtaining passwords can be observed in public, and the compatibility issues to devices arises. Thereby, graphical authentication system called Pass Matrix is used which can be done as one-time login indicator. During the login registration phase the user has to select the set of images. The features of the image will be analyzed and generated the code for each image by using Local Directional Number Pattern (LDN) method which will be stored in the database. The server would generate the pass image from the preselected images (i.e. generate a pass image from the set of images selected by the user during the registration phase.) in which the user has to select the randomly generated pass square during the login phase. To verify whether the generated image is the user selected image or an act of fraudulent.



Fig. 4: A password contains a pass square in an image. The pass square is shown as the orange-filled area in an image.

PassMatrix is composed of the following components (see Figure 5):

- Image Discretization Module
- Login Indicator generator Module
- Communication Module
- Password Verification Module
- Database

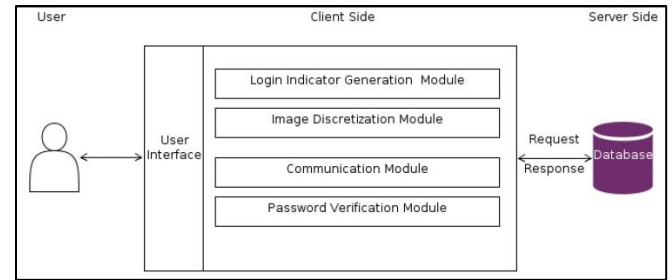


Fig. 5. Overview of the Random Pixel Selection system.

- **Image Discretization Module** This module divides each image into squares, from which users would choose one as the pass-square. An image is divided into a 7x11 grid. The smaller the image is discretized, the larger the password space is.
- **Login Indicator Generator Module** This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) for users during the authentication phase. 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. While generating indicator the features of the image is calculated and generates an LDN code.
- **Communication Module** This module is in charge of all the information transmitted between the client devices and the authentication server. Once an LDN code generated, the code values are compared with the generated LDN code to verify whether the generated image is an original or an act of attacking (Plundering). Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.
- **Password Verification Module** This module verifies the user password during the authentication phase. A pass-square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in pass-image is correctly aligned with the login indicator.
- **Database** The database server contains several tables that store user accounts, passwords (ID numbers of pass images and the positions of pass-squares), and the time duration each user spent on both registration phase and login phase.

#### A. LDN

The Local directional number pattern method encodes the directional information of the image's textures producing a more discriminative code than current methods. We compute the structure of every micro pattern with the support of a compass mask, which extracts directional information, and we encode such information using prominent direction indices and sign, which allows us to distinguish among similar structural patterns that have different intensity transitions. We divide the image into many regions, and extracting the distribution of the LDN features from them.

## IV. CONCLUSION

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a web browser. This link ensures that all data passed between the web server and browsers remain private and integral. The Secure Shell protocol contains numerous features to avoid some of the vulnerabilities with password authentication. Passwords are sent as encrypted over the network, thus making it impossible to obtain the password by capturing network traffic. Also, passwords are never stored on the client. Empty passwords are not permitted by default. On the server side, the Secure Shell protocol relies on the operating system to provide confidentiality of the user passwords. SSH Tectia Server also supports limitation for the number of password retries, thereby making random attacks, brute-force and dictionary attacks difficult. Thereby, different techniques and the input of authenticity can help to secure data. Therefore, by using graphical authentication we can provide a secure system and to be free from fraud and other malpractice.

## REFERENCES

- [1] 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.
- [2] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 236–245.
- [3] 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.
- [4] 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.
- [5] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.
- [6] 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.
- [7] G. Agarwal, S. Singh and R.S. Shukla, "Security Analysis of Graphical Passwords over the Alphanumeric Passwords", in proceedings of the International Journal of Pure and Applied Sciences and Technology, ISSN 2229 – 6107, 2010.
- [8] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200.
- [9] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611–612.
- [10] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "The doodb graphical password database: Data analysis and benchmark results," *Access, IEEE*, vol. 1, pp. 596–605, 2013.
- [11] <http://www.sciencedirect.com/science/article/pii/S0165168412001405>
- [12] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on IEEE Transactions on Dependable and Secure Computing (Volume:PP , Issue: 99 ),09 March 2016 Human Factors in Computing Systems, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2937–2946.
- [13] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–470.
- [14] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical passwordbased user authentication with free-form doodles," *IEEE Transactions on Human-Machine Systems*, vol. PP, no. 99, pp. 1–8, 2015.
- [15] <http://www.internetsociety.org/policybriefs/botnets?gclid=CJKTKqyInNICFdCGaAodMeMETw>
- [16] <https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.WKrQrv197IU>
- [17] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", in proceedings of the IEEE Transactions on Dependable and Secure Computing (Volume: PP , Issue: 99 ), 09 March 2016.