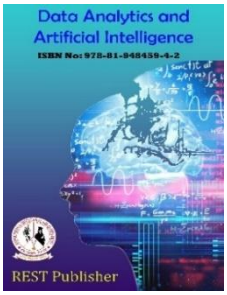
Data Analytics and Artificial Intelligence

Vol: 3(3), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/



Combating Shoulder-Surfing Attacks in Computer Security with a New Graphical Password Technique

Moratanch N, *Ajithkumar P, Bhuanesh Kumar T

Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India.

*Corresponding Author Email: ultiajith1426@gmail.com

Abstract: *One method of computer security authentication is the use of a graphic password. The most crucial aspect of computer science nowadays is digital/computer security, which protects user or client data. And one of the hazards is shoulder-surfing, in which a thief can steal a password by watching directly or by recording the authentication session. The most popular and straightforward way for this authentication is the graphic password strategy. So, to address this issue, we propose a novel strategy. In order to defend against shoulder surfing attacks, we have created two ideas. If there isn't already a registration, the user must first create one. For registration the user has to provide the details such as user name, e-mail id and mobile number. Then, the user has to select image categories. After selecting the categories, the user has to select an image from each category. Hence the registration is done. While login the user has to select the same image category and the images in the same sequence order that has selected while register. To the user, it is given only 3 attempts to select the image. If the user forgets the password, then the user can use email verification for password recovery and password reset. The novel graphical password authentication method that is suggested here is hence resistant to shoulder surfing and other likely attacks.*

Keywords: *Graphical password, image-based authentication, difficult to guess, easy to remember, simple to use.*

1. INTRODUCTION

A pattern password is one of the authentication processes in a computer system. Computer security creates a safe area for digital devices. A graphic password is one of the processes to protect digital devices or information important to us. As you know, the human brain can easily store or remember images or image-based passwords. Therefore, it is recommended to use the image password with high security that can be saved arbitrarily, and there is no problem with withdrawing the photo password. Authentication is the data access point that governs consumer security assurances. This is an acceptable process in the specific context required by the client. Authentication methods are divided into token-based authentication, biometric authentication, and knowledge-based authentication. Tokens are used as private keys in token-based authentication. As the name suggests, it uses images as passwords. Furthermore, scientists claim that images are easier for the human brain to remember than words. The human brain can easily process images. Picture Base Password is strong against dictionary attacks, key loggers, social engineering, and more. Alphanumeric passwords are the traditional and popular method of authentication. This traditional method is too risky for your system. For example, if a user does not use a strong password, an attacker can easily guess the user's password. The user can use Email verification which is a widely used method for password recovery, where a password reset link is sent to the user's email address. This simple yet effective method ensures the security of online accounts by verifying the identity of users. Users can use the same password for multiple devices or sites. To the user, it is given only 3 attempts to select the image. If the user forgets the password, then the user can use email verification for password recovery and password reset. This is a risky feature for normal users. Authentication is one of the important points of security, and users take active responsibility for the security of their personal information.

2. RELATED WORK

Graphical password authentication is a type of password system that uses images or visual elements instead of traditional alphanumeric characters to authenticate users. [1] Although the graphical password technique has the potential to significantly alter how safe a regular user's password might be, it still has some drawbacks. A graphical password technique could be vulnerable to shoulder surfing, which is one of its drawbacks. A graphical password might be physically witnessed, especially in public locations, and if the attacker gets a clear visual of the password being inserted for several times, they could easily crack the password, which is a serious weakness. An alphanumeric password would have a password field just like that. A graphical password strategy's vulnerability to guessing is another possible drawback. Identical to an alphanumeric password if the person only registered.

[2] A graphical password is an authentication method that asks the user to choose from a set of images that are given to them in a certain order via a graphical user interface (GUI). It has been established that this approach has serious disadvantages. For instance, users frequently choose passwords that are simple to guess. On the other side, a password that is difficult to guess is frequently also difficult to remember. In this article, we undertake a thorough analysis of the available graphical password algorithms and suggest a brand-new method. We go over the benefits and drawbacks of each approach while also outlining potential future lines of inquiry

[3] When using touchscreens on mobile devices, it can be difficult to type text passwords, and this problem is getting worse as more people use mobile devices. For usage with touchscreens, we created a brand-new graphical password system called Touchscreen Multi-layered Drawing (TMD). With 31 users, we conducted an exploratory user study of three already-existing graphical passwords for tablets and smartphones. As a result, we decided that one of the design objectives for TMD would be to handle input accuracy difficulties without requiring users to memorise images while keeping a password space that is sufficiently safe. Warp cells, a design feature, enable TMD users to constantly sketch their passwords over many layers, enabling them to build passwords that are more complicated than would often be possible on a small screen. We contrasted TMD's and Draw A Secret's usability.

[4] An image-based enhancement of the password authentication system is proposed in this paper. The graphical password system concept is the primary focus of this paper. The use of cued click points for authentication backs it up. The user's interaction with a sequence of five images is the system's basic idea. This system's primary objective is to improve security by making it easier for users to use and harder for hackers to guess. The best alternative to a text password authentication system is a graphic password. The best alternative to the old graphical password system is the cued click point (CCP) [1]. CCP consists of five click points on five distinct images. In this paper, CCP is paired with emerging technologies like email and mobile phones.

[5] Considering that phishing is a consistently expanding issue, a superior confirmation framework is required. A system that we propose makes use of a graphical password that is entered from an embedded device that is immune to viruses and Trojans. A personal image is used to create the graphical password's image hash, which is then fed into a cryptosystem to generate a password. The user must select a small number of points on the image in order to use the graphical password. These points will then be stretched by the embedded device into a lengthy alphanumeric password. From their individual embedded device, the user can generate numerous passwords with a single graphical password. The device's image hash algorithm was found to be able to respond to minute changes in the underlying image and produce random and unique 256-bit message digests. In addition, it was discovered that the device produced passwords with entropy significantly higher than that of typical user passwords.

[6] Passwords offer an authentication security mechanism and shield services from unauthorised access to resources. One prospective replacement for text-based passwords is a graphical password. Human psychology holds that people can recall images quickly. In this research, we present a new hybrid graphical password-based system that combines algorithms for recognition and recall. This system has numerous advantages over current systems and could be more user-friendly. Our system defends against shoulder surfing and numerous other graphical password assaults. This plan is suggested for smart mobile devices, which are more portable and practical to use than conventional desktop computer systems (such as smart phones, such as the iPod, iPhone, PDAs,etc.)

3. PROPOSED SYSTEM

As the name suggests, different types of images or shapes are used as a password. In addition, a scientist says that human brain can easily store images than text. The human brain can easily process images. so, engineers offered a graphical password authentication system which is very simple to use and very simple to recall their password. And graphical passwords are more secure than text-based password which is resistance of dictionary attack, keyloggers, social engineering etc. In general, graphical password techniques are two types: recognition-based

and recall-based graphic passwords. In graphical password we used 2 types of authentications first is category-based and second is image-based authentication, which is easy to recall and difficult to guess and it is the best alternative to the text password. Humans are visual creatures that process and remember visual clues better than most other forms of data, and graphical passwords exploit just that graphical password, user can easily remember so, no need to write down any password to anywhere. And it is very difficult to guess graphical password.

***3.1 System Architecture*:** The process of graphical password authentication involves the user selecting an image or series of images to create a unique password. The password is stored in a database on a server and encrypted for security. When the user logs in, the authentication system verifies the password by comparing it with the stored password. If the password is correct, access is granted.

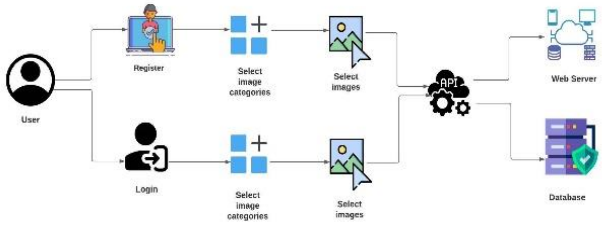


FIGURE1. System Architecture

3.2 Modules: In the module 1, the user has to select at least 3 image category and has to select at least 1 image from each category for successful registration.

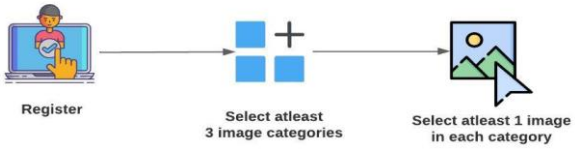


FIGURE 2. Registration Flow

In the module 2, while login the user has to select the categories and images in the correct sequence that has been selected during registration.

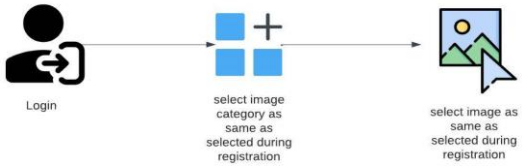


FIGURE 3. Login Flow

4. RESULT

Graphical password authentication provides an alternative and potentially more user-friendly approach to traditional alphanumeric passwords. However, it is important to carefully evaluate the security and usability of any graphical password system before implementing it in a real-world setting.

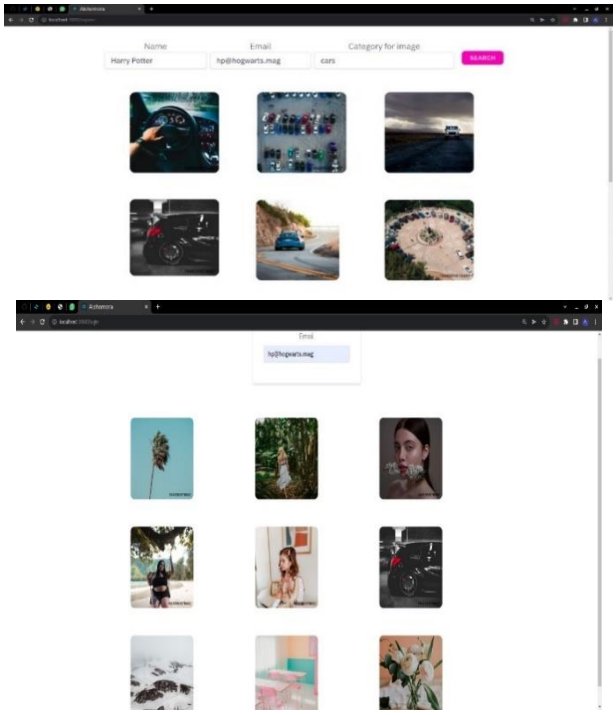


FIGURE 4.

5. CONCLUSION

Using a graphic password as a form of authentication in computer systems can provide improved security compared to traditional alphanumeric passwords. This is because images are easier for the human brain to remember and can be made more secure by using unique and complex patterns. However, it is important for users to take active responsibility for the security of their personal information by using strong passwords and updating them regularly. Additionally, it is recommended to use a combination of authentication methods, such as token-based authentication or biometric authentication, for added security. The goal of authentication is to provide secure access to information and devices, and it is important to choose the best methods to meet the specific needs and context of the user.

REFERENCES

[1]. Alavi, R., Islam, S., Mouratidis, H. & Lee, S., 2015. Managing Social Engineering Attacks- Considering. Proceedings of the Ninth International Symposium on, pp. 161-172.

[2]. Bhanushali, A. et al., 2015. Comparison of Graphical Password Authentication. International Journal of Computer Application, 116(1), pp. 11-15.

[3]. Chavan, S., Gaikwad, S., Parab, P. & Wakure, G., 2015. Graphical Password Authentication System. International Journal of Computer Science and Mobile Computing, 4(4), pp. 324-329.

[4]. CSO, 2017. Hacked Passwords cause 81% of data breaches. [Online] Available at: https://www.cso.com.au/mediareleases/ 29642/hackedpasswords-cause-81-of-data-breaches/ [Accessed 19 May 2018].

[5]. Gao, H., Jia, W., Ye, F. & Ma, L., 2013. A Survey on the use of Graphical Passwords in Security. Journal of Software, 8(7), pp. 1678-1698.

[6]. Gokhale, A. & Waghmare, V., 2013. Graphical Password Authentication Techniques. International Journal Science and Research, 4(7), pp. 279-285.

[7]. Khan, W.Z., Aalsalem, Y.M. & Xiang, Y., 2011. A Graphical Password Based System for Small Mobile Devices. International Journal of Computer Science Issues, 8(5), pp. 145-155.

[8]. Kumar, E. & Bilandi, E.N., 2014. A Graphical Password Based Authentication Based System for Mobile Devices. International Journal of Computer Science and Mobile Computing, 3(4), pp. 744-754.

[9]. Leonardo Sobrado, J.C.B., n.d. Graphical passwords. The Rutgers Scholars, Volume 4, pp. 1-8.

[10]. Mayer, A., Monrose, F. & Reiter, M.K., 2011. The Design and Analysis of Graphical Passwords. New York University, pp. 1-14.

[11]. Parkinson, M., 2016. The Power of Visual Communication. [Online] Available at: http://businesscommunicationnetwork. com/wpcontent/plugins/BNet/cache/1327279949.html [Accessed 19 May 2018].
[12]. Perrig, A. & Dhamija, R., 2011. Deja Vu: A User Study Using Images for Authentication. SIMS / CS, University of California Berkeley, p. 14.
[13]. Shraddha S. Banne, P.N., 2012. A review of the graphical password based authentication Schemes. International Journal of Science and Research, 2319-7064(3.358), pp. 1-3.
[14]. Towseef Akram, V.A.E., 2017. Graphical Password Authentication. International Journal of Computer Science and Mobile Computing, 6(6), pp. 394-400.
[15]. Shrivastava, S., Jeyanthi, P.M. and Singh, S., 2020. Failure prediction of Indian Banks using SMOTE, Lasso regression, bagging and boosting. Cogent Economics & Finance, 8(1), p.1729569.

