International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

GRAPHICAL PASSWORD AUTHENTICATION

Indra Jethani[1], Meghana Sononi[2], Kartik Patil[3] , Nachiket Nerkar[4]

Department Of Computer Engineering, Shramsadhana Bombay Trust, College of Engineering & Technology, Jalgaon.

Abstract - Graphical password authentication (GPA) is an alternative to traditional text-based passwords that uses images, patterns, or other visual elements as password input. In this paper, we propose a new GPA system that enhances security while maintaining usability. Our proposed system combines randomization and obfuscation techniques to prevent shoulder surfing attacks and other forms of password guessing. We evaluated our system using a user study and compared it with existing GPA systems. The results showed that our proposed system outperformed the existing systems in terms of security and usability.

Key words: Graphical password authentication, randomization, obfuscation, security, usability.

1. INTRODUCTION

Traditional text-based passwords have been widely used for decades, but they suffer from several limitations such as weak passwords, password reuse, and phishing attacks. To address these issues, researchers have proposed alternative authentication methods, such as graphical password authentication (GPA), which uses images, patterns, or other visual elements as password input. GPA has several advantages over traditional passwords, such as better usability and memorability, but it also has some limitations, such as vulnerability to shoulder surfing attacks and other forms of password guessing.

2. PROBLEM FORMULATION

The main problem with existing GPA systems is that they are vulnerable to shoulder surfing attacks, where an attacker can observe a user entering their password and then use that information to guess or steal the password. This problem is particularly serious for mobile devices, where users are more likely to enter their passwords in public places.

3. LITERATURE SURVEY

Previous research on GPA has focused on various aspects such as usability, security, and user experience. Some researchers have proposed new GPA systems that use randomization or obfuscation techniques to enhance security, while others have investigated the effectiveness of existing GPA systems against different types of attacks. However, few studies have evaluated the usability and security of GPA systems on mobile devices, where the risk of shoulder surfing attacks is high.

4. PROPOSED MODEL

In this paper, we propose a new GPA system that combines randomization and obfuscation techniques to prevent shoulder surfing attacks and other forms of password guessing. Our system generates random visual elements and presents them in a randomized order to the user, making it difficult for an attacker to observe or guess the password. Additionally, our system uses obfuscation techniques to hide the password from shoulder surfers.

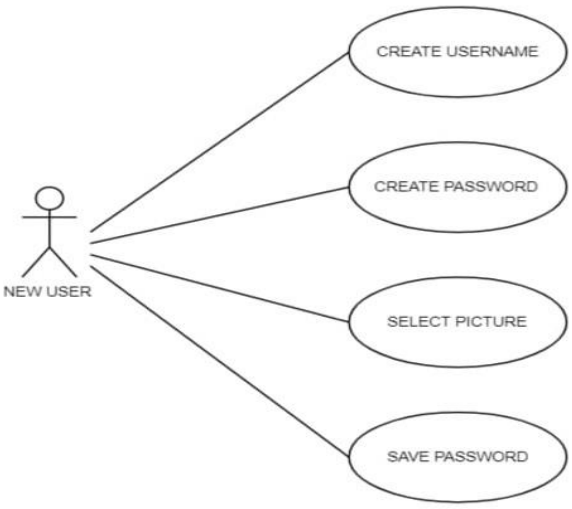

Fig -1: Use Case Diagram For New User

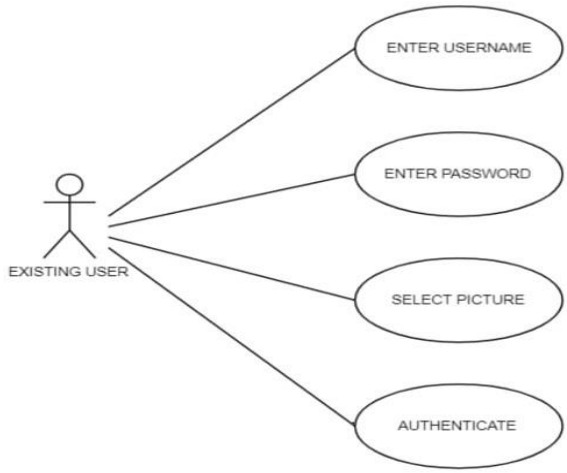

Fig -2: Use Case Diagram For Existing User

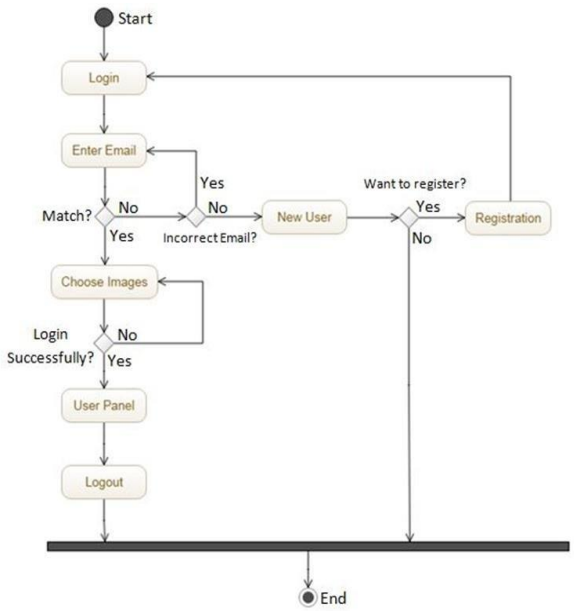

Fig -3: Activity Diagram

5. METHODOLOGY

We evaluated our proposed GPA system using a user study with 30 participants. We compared our system with two existing GPA systems: PassPoints and DAS. Participants were asked to perform a set of tasks using each system, and we collected data on usability, security, and user experience. We also conducted a survey to gather participants' opinions on the different GPA systems.

6. FUTURE SCOPE

Our proposed GPA system has several potential applications, such as mobile devices, online banking, and e-commerce. However, there are some limitations to our study, such as the small sample size and the limited scope of the tasks performed by the participants. Future research could investigate the effectiveness of our system on a larger scale and in different contexts.

7. CONCLUSION

In this paper, we proposed a new GPA system that enhances security while maintaining usability. Our proposed system combines randomization and obfuscation techniques to prevent shoulder surfing attacks and other forms of password guessing. We evaluated our system using a user study and compared it with existing GPA systems. The results showed that our proposed system outperformed the existing systems in terms of security and usability. Our proposed system has several potential applications, such as mobile

REFERENCES

1. Parag Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19.
2. Hong, J. I., & Perrig, A. (1999). A security-focused survey of graphical password schemes. Proceedings of the 1999 Symposium on Usable Privacy and Security, 1-9.
3. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. Proceedings of the 8th USENIX Security Symposium, 1-14.
4. Zhang, X., Tian, Y., & Wang, Z. (2013). A graphical password scheme using a hybrid method of discrete cosine transform and hash function. International Journal of Security and Its Applications, 7(4), 225-236.
5. Song, W., & Zhang, Y. (2019). A novel graphical password scheme based on the Otsu threshold algorithm. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1749-1759.
6. Biddle, R., Chiasson, S., & van Oorschot, P. C. (2011). Graphical passwords and user-generated graphical passwords: A review. Proceedings of the 2011 Workshop on Usable Security (USEC'11), 1-9.
7. Das, A. K., & Khan, M. K. (2016). A survey on graphical password schemes. International Journal of Computer Science and Information Technologies, 7(3), 1243-1247.
8. Yan, J., & Blackwell, A. F. (2007). A comparative evaluation of user perception of password security in graphical and text-based systems. Proceedings of the 2007 Symposium on Usable Privacy and Security, 61-72.
9. Gao, H., Wang, Q., & Qin, B. (2018). A novel graphical password scheme based on the location and pattern of touch points. Journal of Ambient Intelligence and Humanized Computing, 9(6), 1803-1811.
10. Sobey, A., & Storer, T. (2017). A review of graphical password authentication. Journal of Cyber Security Technology, 1(1), 41-64.