Educational Administration: Theory and Practice
2023, 29(2), 686 - 688
ISSN: 2148-2403
https://kuey.net/
Research Article

Secure Graphical Password Authentication

Anil H Rokade[1*], Santosh S. Lomte[2], Waseem Shaikh[3], Ojas Joshi[4]

[1*]Asst.Professor, Deogiri Institute of Engineering and Management Studies, Place: Aurangabad (Chh. Sambhajinagar), Email id: anilrokade@dietms.org
[2]Principal, Dr. BAMU, Aurangabad (Chh. Sambhajinagar), Email id: drsantoshlomte@gmail.com
[3]Student, Deogiri Institute of Engineering and Management Studies, Aurangabad (Chh. Sambhajinagar)
Email id: waseemshaikh3004@gmail.com
[4]Student, Deogiri Institute of Engineering and Management Studies, Aurangabad (Chh. Sambhajinagar)
Email id: ojaspjoshi1729@gmail.com

Citation: Anil H. Rokade, et al. (2023), S Secure Graphical Password Authentication, *Educational Administration: Theory and Practice*, 29(2) 686 - 688
Doi: 10.53555/kuey.v29i2.8404

ARTICLE INFO **ABSTRACT**

The goal of this study is to present a novel graphical password system that enhances both security and usability. Using a 6x6 grid with dynamic number associations for each login session, the system is resistant to observation and brute-force attacks. User surveys show that this system is highly memorable and error-free, indicating potential for real-world applications in high-security environments.

Keywords: Graphical Authentication, Security, Usability, Dynamic Password, Authentication, Secure Model

Introduction:

• **Background and Context:**Traditional text-based passwords are widely used for authentication but suffer from significant security and usability issues. They are prone to brute-force, phishing, and observation attacks, and are often difficult for users to remember.
• **Research Question:**Can a dynamic graphical password model improve security and usability over traditional text-based and static graphical passwords?
• **Significance of the Research:** Developing an authentication method that balances security with usability is crucial, especially for high-security applications that require user-friendly access controls.
• **Paper Structure:** This paper includes a review of relevant literature, a description of the methodology, presentation of results, discussion of findings, and concludes with implications and future directions.

Literature Review:

• **Review of Relevant Literature:**Prior research has explored various authentication mechanisms, such as text-based passwords, biometrics, and static graphical passwords. Text-based methods are known for poor memorability, while biometrics introduce privacy concerns.
• **Existing Theories and Gaps:**While static graphical passwords improve memorability, they often lack dynamic elements, making them vulnerable to shoulder surfing and other attacks. Dynamic approaches in authentication have been less explored.
• **Justification for the Current Study:**This study addresses a key gap by developing a dynamic graphical password model that adapts with each session, enhancing resistance to various attacks without compromising user ease of access.

Methodology:

• **Research Design:**This study employs a mixed-methods approach, combining quantitative assessments with qualitative user feedback.
• **Data Collection Methods:**The system was tested with user participants who used the graphical password system. Surveys were conducted to assess usability, and simulated attacks (brute force, shoulder surfing, spyware, and phishing) were performed to test resistance.

• **Data Analysis Techniques:**Statistical analysis was used to compare the system’s performance across different attack types, while qualitative analysis of user feedback provided insights into memorability and ease of use.

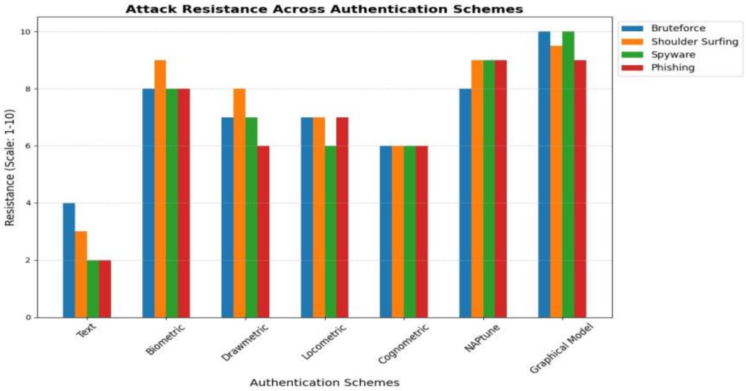
Results:

• **Findings Presentation:**

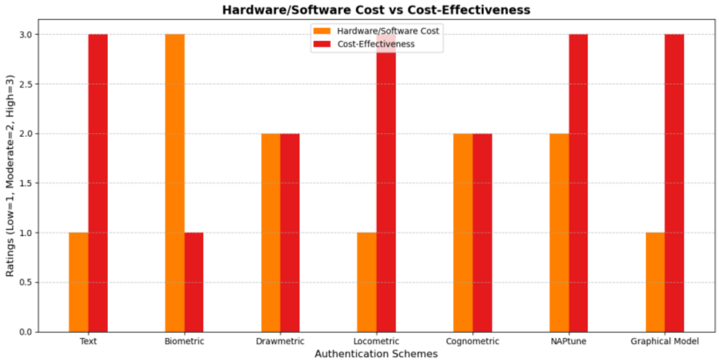
- **Attack Resistance:** The dynamic graphical password model showed high resistance to brute force, shoulder surfing, spyware, and phishing attacks, as demonstrated in Figure 1.
- **User Error Rates:** User error rates were low, indicating that the system is user-friendly and easy to remember.
- **User Feedback:** Participants expressed satisfaction with the system's ease of use and the dynamic nature of the passwords.

• **Visual Aids:**

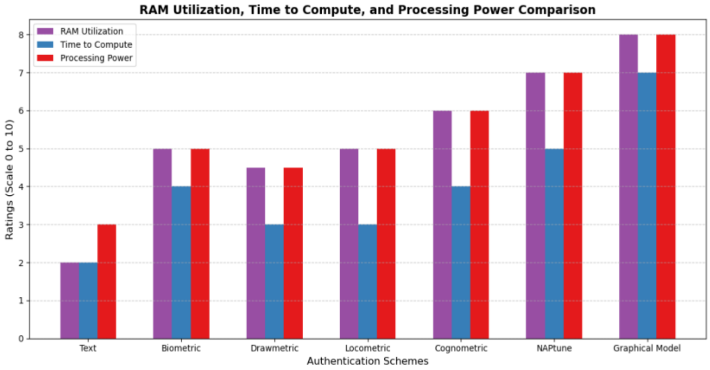
- **Figure 1:** Attack Resistance Across Authentication Schemes



- **Figure 2:** Hardware/Software Cost vs. Cost-Effectiveness



- **Figure 3:** RAM Utilization, Time to Compute, and Processing Power Comparison



Discussion:

- **Interpretation of Results:**The high resistance scores across various attack vectors confirm the effectiveness of the dynamic graphical model in enhancing security.
- **Comparison with Previous Research:**Unlike traditional static graphical models, this system shows improved security without sacrificing usability, aligning with recent advancements in adaptive authentication.
- **Implications:**This model can be particularly beneficial for high-security applications where both security and user accessibility are essential.
- **Limitations and Future Research:**Real-world deployment and testing are necessary to validate findings. Future studies could explore integrating this system with multi-factor authentication for even greater security.

Conclusion:

- **Summary of Key Findings:**The dynamic graphical password model offers high security and usability, outperforming traditional methods in attack resistance and user satisfaction.
- **Broader Significance:**This system provides a promising alternative to traditional passwords, addressing both security and memorability challenges.
- **Practical Applications:**This model could be implemented in secure applications that prioritize user-friendly access, such as financial services and corporate environments.

Acknowledgement:

Our sincere appreciation to Dr. Santosh S. Lomte for his essential counsel during this study project. Furthermore, we would like to thank the content curator, Waseem Shaikh, for his careful work in compiling and arranging the information in this study. Particular gratitude is owed to Ojas Joshi for his technical assistance, which was indispensable during the stages of development and testing.

Conflict of Interest:

The authors declare no conflicts of interest related to this study.

References:

[1] Adams, A., and Sasse, M. A. 1999. Users are not the enemy. Commun. ACM, 42(12), 40-46.

[2] Bedworth, M. A. Theory of Probabilistic One-Time Passwords. Retrieved from http://www.pinoptic.com/downloads/wp002_a_theory_of_potp.pdf

[3] Brostoff, S., and Sasse, M. A. Are Passfaces more usable than passwords? A field trial investigation. In Proceedings of HCI on People and Computers XIV (HCI 2000), 405-424.

[4] Brostoff, S., Inglesant, P., and Sasse, M. A. Evaluating the usability and security of a graphical one-time PIN system. BCS Conference on Human-Computer Interaction, Dundee, Scotland, 6-10 Sep 2010.

[5] Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 1-41.

[6] Bonneau, J. (2012). The science of guessing: Analyzing an anonymized corpus of 70 million passwords. IEEE Symposium on Security and Privacy, 538-552.

[7] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 553-567.

[8] Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. Proceedings of HCI 2000, 405-424.

[9] Oorschot, P. C. (2009). A second look at the usability of click-based graphical passwords. Proceedings of the 3rd Symposium on Usable Privacy and Security, 1-12

[10] Dhamija, R., & Perrig, A. (2000). Déjà Vu: A user study using images for authentication. Proceedings of the 9th USENIX Security Symposium, 45-58.

[11] Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS),

[12] Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. Proceedings of the 16th International Conference on World Wide Web, 657-666

[13] Thorpe, J., & van Oorschot, P. C. (2007). Human-seeded attacks and exploiting hot-spots in graphical passwords. Proceedings of the 16th USENIX Security Symposium.