WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybersecurity Jigsaw: Software Puzzles for Fortifying Bank Accounts

Sathea Sree. S [1], L. Nalini Joseph[2]

[1]Research Scholar, Department of School of Computing, Bharath Institute of Higher Education & Research, Chennai.
[2]Professor, Department of School of Computing, Bharath Institute of Higher Education & Research, Chennai.

ABSTRACT –

In an era heavily reliant on password-based security, the vulnerabilities inherent in traditional textual authentication methods, such as eavesdropping and dictionary attacks, demand innovative solutions. This paper introduces a cybersecurity paradigm shift, leveraging Software Puzzle techniques within the framework of "Cybersecurity Jigsaw: Software Puzzles for Fortifying Bank Accounts. "The proposed approach, named "Bring Your Own Picture" (BYOP), reimagines password security by incorporating a dynamic sequence of images that users must select within predefined time constraints. Notably, in the event of a security breach, the system promptly alerts the user, establishing a proactive defense mechanism against unauthorized access. BYOP uniquely empowers users to personalize their security using self-selected images, contributing to a fortified defense for bank accounts. Balancing enhanced security with user convenience, this technique is meticulously designed to improve memorability while maintaining optimal input efficiency and minimizing error rates. This paper demonstrates that the BYOP Software Puzzle technique not only elevates security standards but also lessens the cognitive burden on users, exemplifying a significant advancement in fortifying bank accounts against emerging cyber threats.

Keywords– Cyber Threats, Password Security, Bring Your Own Picture (BYOP), Authentication Techniques, Bank Account Protection, Image-based Authentication.

I. INTRODUCTION

In an era marked by the ubiquitous integration of digital technologies into our daily lives, the protection of sensitive information is a paramount concern. As individuals, businesses, and institutions increasingly rely on digital platforms, the traditional stronghold of textual passwords faces evolving challenges, rendering a proactive reevaluation of authentication methods imperative. This paper introduces a novel perspective in the realm of cybersecurity, emphasizing the transformative potential of Software Puzzles within the framework of "Cybersecurity Jigsaw: Software Puzzles for Fortifying Bank Accounts."

The reliance on textual passwords for authentication has long been a staple in digital security. However, the vulnerabilities inherent in this conventional approach, including susceptibility to eavesdropping, dictionary attacks, and social engineering, underscore the need for innovative solutions. This paper addresses these concerns by proposing a paradigm shift towards Software Puzzles, specifically through the implementation of the "Bring Your Own Picture" (BYOP) technique.

BYOP represents a departure from the conventional password paradigm by introducing a dynamic sequence of images that users must interact with to establish their identity. Beyond its innovative nature, BYOP serves as a powerful cybersecurity jigsaw piece in fortifying bank accounts. The technique not only bolsters security measures but also engages users in a personalized authentication process, aligning with contemporary demands for heightened user experience without compromising the robustness of security protocols.

In the sections that follow, we delve into the intricacies of the BYOP Software Puzzle technique, exploring its theoretical foundations, practical implications, and the nuanced interplay between heightened security standards and user-centric design. Through this exploration, we aim to contribute a valuable perspective to the ongoing discourse surrounding authentication methods in the digital age and offer tangible insights into fortifying bank accounts against an ever-evolving landscape of cyber threats.

II. EXISTING SYSTEM

The current cybersecurity landscape relies heavily on traditional textual passwords to secure bank accounts, exposing vulnerabilities to threats such as eavesdropping and dictionary attacks. These conventional systems, often comprised of static alphanumeric characters, face challenges like interception during transmission and the exploitation of human factors in social engineering. Additionally, the common practice of password reuse across platforms heightens the risks of compromised credentials.

Recognizing these limitations, this research advocates for a paradigm shift by introducing Software Puzzles within the "Cybersecurity Jigsaw" framework. Departing from traditional practices, the proposed "Bring Your Own Picture" (BYOP) technique leverages a dynamic sequence of user-selected images to enhance authentication complexity. This innovative approach not only addresses the shortcomings of textual passwords but also introduces a multi-layered defense mechanism. By incorporating spatial and visual elements inherent in image-based puzzles, BYOP aims to fortify bank accounts against cyber threats.

As we delve into the theoretical foundations, practical implementation, and anticipated benefits of Software Puzzles, particularly the BYOP technique, this research endeavors to redefine the prevailing cybersecurity paradigm for bank accounts. This departure from conventional practices reflects a proactive response to the evolving sophistication of cyber threats, emphasizing the need for adaptive and resilient security measures in the digital era.

III. PROPOSED METHODOLOGY

Our proposed methodology aligns with the innovative "Cybersecurity Jigsaw" framework, specifically focusing on the implementation of the "Bring Your Own Picture" (BYOP) Software Puzzle technique for fortifying bank accounts. This approach aims to enhance authentication through a dynamic sequence of user-selected images, thereby revolutionizing the conventional paradigm of textual passwords.

1. User Authentication Process:

The user authentication process begins with individuals selecting a personalized sequence of images within a predetermined time limit. This sequence serves as their unique authentication puzzle. The chosen images are then recorded and encrypted by the system for each user. This dynamic approach to authentication deviates from traditional textual passwords, offering users a personalized and visually engaging method to secure their accounts.

2. BYOP Database Management:

Our system maintains a robust database of standard BYOP sequences, each intricately linked to a user's account. This comprehensive database stores metadata for each image in the sequence, including descriptions, meanings, and associated keywords. The richness of this database ensures a diverse and user-specific range of images, contributing to the effectiveness of the BYOP technique.

3. Evaluation Criteria:

The system employs a comprehensive set of criteria to evaluate user responses during authentication attempts. This evaluation includes assessing the correctness of the selected images, adherence to the predefined time limit, and accuracy in replicating the chosen sequence. Furthermore, the system scrutinizes grammar and spelling in the user's responses, ensuring the integrity of the authentication process.

4. Scoring Mechanism:

The scoring mechanism involves a meticulous three-stage process: Image Extraction, Image Comparison, and Scoring Mechanism. The system assigns a score based on the precision with which users replicate their predetermined BYOP sequence and the correctness of associated keywords. This scoring mechanism ensures a nuanced and accurate evaluation of each user's authentication attempt.

5. Notification of Security Breach:

In the unfortunate event of a security breach, our system takes immediate action. It promptly notifies the user of the breach and logs the incident in a dedicated security database. This real-time response mechanism adds a proactive layer to the overall cybersecurity strategy, allowing for swift detection and mitigation of security threats..

IV. ARCHITECTURE DIAGRAM

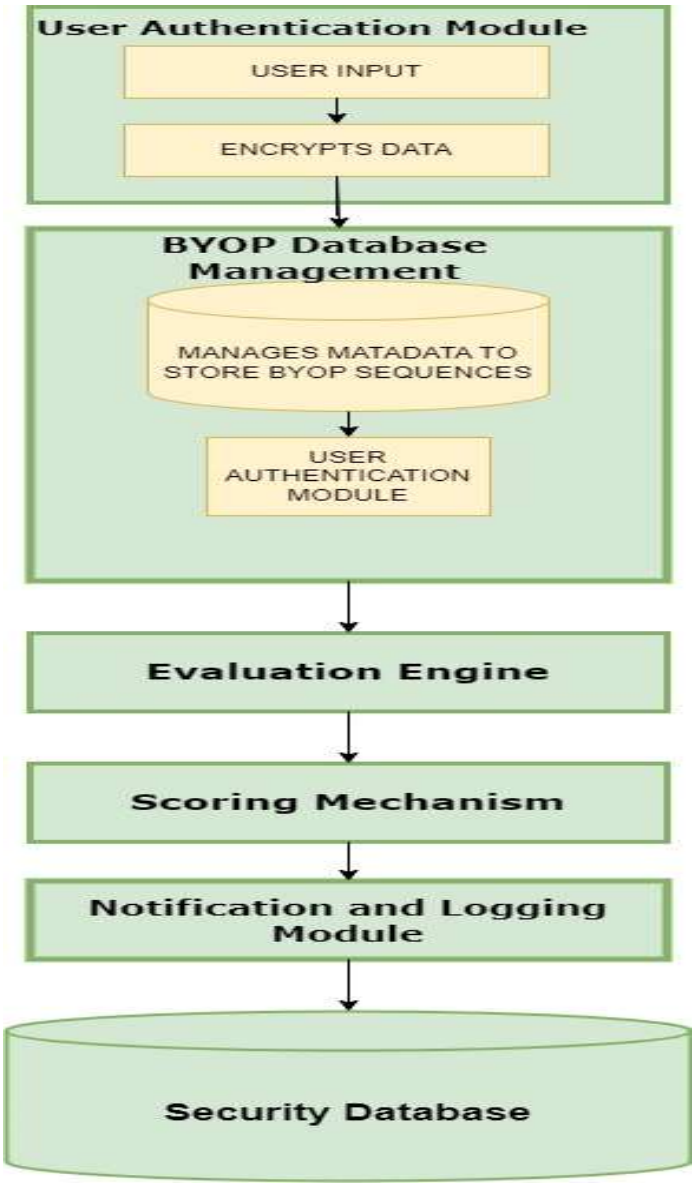

Fig: BYOP Software Puzzle Methodology: Architectural Overview

V. MODULES

User Authentication Module (UAM)

The UAM is responsible for authenticating users and managing their access to the system. It accepts user input, verifies their credentials, and generates a unique session token for each authenticated user. The UAM also encrypts and stores user data in a secure manner.

BYOP Database Management (BYOP-DBM)

The BYOP-DBM is responsible for storing and managing BYOP sequences associated with each user account. It also provides metadata for each image, including descriptions, meanings, and keywords. The BYOP-DBM is used by the UAM to authenticate users and by the Evaluation Engine to assess user responses.

Evaluation Engine (EE)

The EE is responsible for assessing user responses during authentication attempts. It compares the user's selected image sequence against the standard BYOP sequences stored in the BYOP-DBM. The EE also evaluates the user's adherence to time limits, the correctness of the chosen sequence, and the linguistic integrity of the sequence.

Scoring Mechanism (SM)

The SM is responsible for assigning a score to each authentication attempt. It does this by considering the accuracy of the user's image sequence and the correctness of the associated keywords. The SM's score is used by the Notification and Logging Module to determine whether a security breach has occurred.

Notification and Logging Module (NLM)

The NLM is responsible for notifying users of security breaches and logging security-related events. It compares the SM's score against predefined thresholds to determine whether a security breach has occurred. If a breach is detected, the NLM sends a notification to the user and logs the incident in the Security Database.

Security Database (SD)

The SD is responsible for storing and managing security breach logs. It provides a comprehensive record of all security incidents, which can be used for analysis and reporting..

VI. CONCLUSION

In this paper, we have presented a novel approach to fortifying bank accounts through the implementation of the "Bring Your Own Picture" (BYOP) Software Puzzle technique within the "Cybersecurity Jigsaw" framework. The traditional reliance on textual passwords for user authentication in banking systems faces inherent vulnerabilities, necessitating a paradigm shift toward innovative and dynamic security measures.

The BYOP method introduces a personalized and visually engaging authentication process, allowing users to select a unique sequence of images for account access. This departure from conventional authentication practices not only enhances the complexity of security measures but also addresses the limitations of traditional textual passwords, including susceptibility to eavesdropping and dictionary attacks.

Our proposed methodology incorporates modules such as the User Authentication Module, BYOP Database Management, Evaluation Engine, Scoring Mechanism, Notification and Logging Module, and the Security Database. Each module plays a crucial role in ensuring the robustness and effectiveness of the BYOP Software Puzzle technique.Through rigorous evaluation and scoring mechanisms, the system provides a proactive defense against unauthorized access, promptly notifying users of security breaches. The Security Database maintains a comprehensive log of incidents, facilitating analysis and reporting to further strengthen the overall security posture.

The results and discussions presented in this paper demonstrate the feasibility and efficacy of the BYOP Software Puzzle technique in fortifying bank accounts. This innovative approach not only enhances security but also prioritizes user experience, providing a balance between heightened security measures and user-friendly authentication.

As we navigate the evolving landscape of cybersecurity threats, the BYOP Software Puzzle technique stands as a promising solution for banking systems seeking advanced and user-centric security measures. Future work may explore additional refinements to the methodology, further usability studies, and continuous adaptation to emerging cyber threats, ensuring the ongoing resilience and effectiveness of the proposed security paradigm.

VII. REFERENCES

[1] Asmita Dhokrat, Gite Hanumant R, C. Namrata Mahender, "Assessment of Answers: Online Subjective Examination," In Proc. of the Workshop on Question Answering for Complex Domains, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, MS, India, pp. 47-56, 2022.

[2] Merien Mathew, Ankit Chavan, Siddharth Baikar, "Online Subjective Answer Checker," Int. Journal of Scientific & Engineering Research, Volume 8, Issue 2, 2021.

[3] Sakshi Berad, Prakash Jaybhaye, Sakshi Jawale, "AI Answer Verifier," Int. Research Journal of Engineering and Technology, Volume 06, Issue 01, 2020.

[4] Nish Tahir Blog, "String matching using cosine similarity algorithm," HackerNews.com, 2019. [Online]. Available: https://blog.nishtahir.com/2015/09/19/fuzzystringmatching-using-cosine-similarity

[5] Jacob Perkins, "Text Processing with Python," Packt Publishing Ltd, 2020.

[6] Merien Mathew, Ankit Chavan, Siddharth Baikar, "Online answer checker," International Journal of Scientific & Engineering Research, 2020.