Methodology Issue

Mitigating Online Password Attacks: A Comprehensive Review of Password Models

Kirushnaamoni Ramakrishnan

Abstract

Most authentication systems rely on alphanumeric passwords as a first line of defence. This review outlines various online password attacks and evaluates models proposed to mitigate them. A secondary aim is to explore ways to improve password selection and memorability without user inconvenience. Nine articles from 2019 to 2023 were reviewed, focusing on password checkers, entropy values (entropy is a measure of uncertainty), and password structures to ensure system security against online attacks, while analysing usability and security aspects of the models. Most of these models were implemented in controlled environments rather than in real-time scenarios. Future work includes surveying user preferences for password and authentication systems.

Keywords—Online password attacks, Brute force attacks, Dictionary attacks, Cross-site attacks, authentication systems, password-based systems, alphanumeric passwords

Introduction

Authentication is a fundamental component of any system (Barkadehi et al., 2018). Since their introduction in 1961, passwords have evolved from text-based to graphical and combinational forms (Wang et al., 2021). They are convenient, easy to implement, and user-friendly (Kirushnaamoni, 2013). Password authentication relies on the knowledge-based model, where users know the required information. This review examines the challenges of text-based password systems and analyses methods designed to prevent online password attacks.

Search strategy

There are four types of literature reviews: a) Narrative reviews: these reviews focus on the concepts and provide information on the current scenario of the specific research area b) Developmental reviews: based on previous research findings, new and innovative methods and procedures would be suggested by the authors c) Cumulative reviews: offer experimental evidence to support the literature and overall conclusion d) Aggregative reviews: these reviews combine previous findings and examine specific topics within the

broader research area (Barkadehi et al., 2018). The aggregative review type was preferred over the other types of literature reviews as the review focused on previous findings and specific topics in the authentication systems.

The systematic review methodology used for reporting the articles was PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) (Moher, 2019). The search was conducted using four databases: Scopus, SpringerLink, IEEE Xplore Digital Library and Google Scholar. The reasons for choosing these databases are that they provide a wide range of high-quality, relevant sources with up-to-date research findings. The keywords used to search were “Online password attacks” OR “Brute force attacks” OR “Dictionary attacks” OR “Cross-site attacks”, “Passwords” OR “Authentication systems”. Additionally, instead of OR, the Boolean operator AND was also used to conduct searches.

Article selection criteria

An initial screening removed duplicate records, followed by title and abstract reviews to exclude additional records. Full-text articles were then reviewed based on eligibility criteria. The eligibility criteria for including the articles were:

1) Peer-reviewed articles published either as a conference paper or journal article.
2) Papers ranging from 2019 to 2023 were considered for the review.
3) Online password attacks and text-based password models were considered.
4) Papers were selected from areas related to web and computer-based authentication.
5) The article should be written and published in English.

Article exclusion criteria

The criteria for excluding the articles are outlined below:

1) Non-peer-reviewed articles were not considered for the review.
2) Papers related to offline password attacks were not considered.
3) Studies related to graphical passwords or any other type of user authentication like biometrics,

tokens, and smart cards were not included.

Article search results

Initially, 176 research papers were identified. After excluding the duplicate papers, 144 papers were eligible for screening. Based on the initial screening, a total of 81 papers did not meet the inclusion criteria. The remaining 63 papers were included to be evaluated for eligibility, out of which 9 were selected for the final review. The study selection process is depicted in Fig. 1.

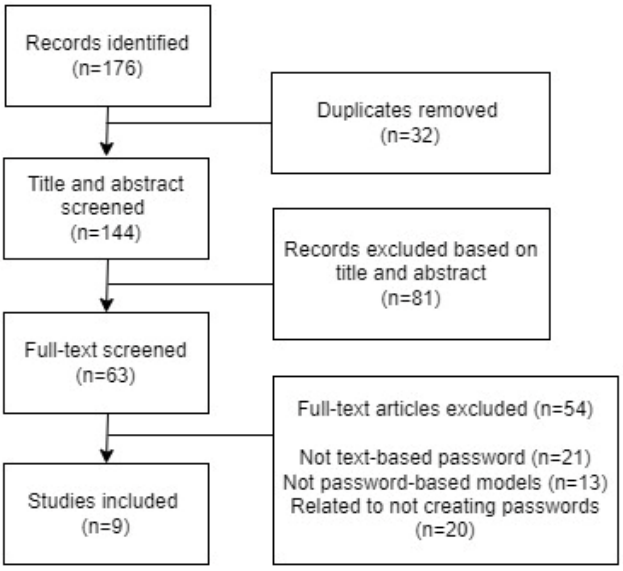

Fig.1 The study selection process

Research questions

Selected papers were first evaluated for the relevance of their title, abstract, and introduction before their full-text version was examined to address the research questions that have been answered throughout this review.

TABLE I. RESEARCH QUESTIONS (RQ)

No.	Research questions
Q1	What are the models developed to identify, reduce, or prevent online passwo attacks?
Q1.1	What are the findings and how are the models evaluated?
Q2	How can the strength of the passwords be improved along with memorability

Scope of review

The scope of this review encompasses algorithms and systems that organizations can implement to analyse user passwords or provide suggestions for creating stronger, more memorable passwords.

Words of wisdom

The primary motivation for this review was to further investigate my paper published 10 years ago. I was curious to see if new methods for creating strong, memorable passwords had emerged and whether ATTs (Automated Turing Tests) were still necessary to prevent unauthorized access. Unfortunately, I could not find enough recent papers on this topic, which forced me to shift my focus midway. Instead of analysing password creation methods, I opted to examine models for combating online password attacks. I was pleased to discover that there were recent publications available, enabling me to complete my research.

For researchers interested in conducting a systematic literature review, I recommend ensuring that a sufficient number of relevant papers are available before beginning the study. If the review encompasses literature from the last 10 or 20 years, this may not pose a problem. However, if it focuses on papers from the past 5 years, like mine, it is crucial to confirm the availability of a substantial body of work. Additionally, identifying the type of literature review being conducted can enhance the reader's understanding of the review's scope and focus.

Conclusion

I initially planned to continue this research for the 60-point dissertation but felt drawn to explore Intrusion Detection Systems instead. In the future, I may revisit this topic, surveying users about: a) password types b) password change frequency c) password manager usage d) password reuse across different sites and e) preferred authentication methods. This would shed light on current password practices and inform the need for more robust authentication methods in organizations.

Short Bio

I am a research master’s student in the field of Computer and Information Sciences under the Faculty of Creative and Design Technologies at Auckland University of Technology. I am also a student ambassador, an RUOK advisor, a volunteer with Conservation Volunteers New Zealand (CVNZ), an entrepreneur, a peer reviewer and a student editor with Rangahau Aranga, which is AUT’s Graduate Review

journal. My research interests include network security, machine learning and bioinformatics.

Acknowledgements

I would like to thank AUT for this opportunity to provide a platform for postgraduate students to submit their work for the journal and experience the joy of seeing their articles getting published. This research was conducted as part of an assessment for the STEM Research paper (ENGE817) in semester 2, 2023, as part of the Master of Computer and Information Sciences program (AK1329) at Auckland University of Technology.

References

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Zakeri Fardi, A., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, *35*(5),1491–1511. https://doi.org/10.1016/j.tele.2018.03.018

Kirushnaamoni, R. (2013, February). Defenses to curb online password guessing attacks. In *2013 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 317-322). IEEE.

Moher, D. (2019). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Annals of Internal Medicine*, *151*(4), 264. https://www.acpjournals.org/doi/abs/10.7326/0003-4819-151-4-200908180-00135.

Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications*, *188*(1), 103080. https://doi.org/10.1016/j.jnca.2021.103080.