Enhancing Digital Security: A Zero-Knowledge Proof-Based Authentication System for User Privacy Protection – Project Proposal

Thomason Zhao
UW–Madison

Thomas Peng
UW–Madison

ABSTRACT

This proposal outlines the development and evaluation of a privacy-preserving authentication system leveraging zero-knowledge proofs to authenticate users without revealing any personally identifiable information.

1 INTRODUCTION

In an era where digital transactions and interactions have become ubiquitous, the significance of robust authentication mechanisms cannot be overstated. The security of online systems heavily relies on the ability to accurately verify the identity of users. Traditional authentication methods [11], which include passwords, security tokens, and biometric systems, aim to balance convenience with security. However, they often fall short when it comes to protecting users' privacy. Personal data breaches, identity theft, and unauthorized surveillance are prevalent issues that stem from the over-exposure of personally identifiable information (PII) during the authentication process [12].

The central dilemma is thus: How can we verify an individual's identity and grant access to services without compromising their privacy by revealing or storing sensitive personal information? This question has sparked considerable interest in the field of cryptography and, more specifically, in the concept of zero-knowledge proofs (ZKPs) [6]. ZKPs are a breakthrough in cryptographic techniques that allow one party (the prover) to prove to another party (the verifier) that a given statement is true, without revealing any information beyond the validity of the statement itself. This can be likened to proving that a key fits a lock without revealing the shape of the key.

The motivation behind this project is to harness the power of zero-knowledge proofs to create a privacy-preserving authentication system. Such a system would enable users to prove their identity or credentials without exposing any PII, thus maintaining their privacy and security. The potential applications of this technology are vast and include sectors where privacy is paramount, such as online banking, secure communications, e-voting systems, and healthcare.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

The challenge we aim to address is: firstly, to design and implement an authentication system that is as intuitive and user-friendly as traditional methods, and secondly, to ensure this system upholds the rigorous security standards required for widespread adoption without incurring prohibitive computational costs.

To achieve this goal, we will need to navigate a landscape where the theoretical possibilities of zero-knowledge proofs intersect with practical limitations. We will explore the latest advancements in zero-knowledge protocols, such as zk-SNARKs (zero-knowledge Succinct Non-interactive Arguments of Knowledge) [4, 10] and zk-STARKs (zero-knowledge Scalable Transparent Arguments of Knowledge) [1, 2] and investigate how these can be optimized for real-world authentication scenarios. This exploration will include addressing potential scalability issues and reducing the computational overhead to facilitate a seamless user experience.

Our project, therefore, stands at the intersection of cryptography, software engineering, and usability design. It is poised to make a significant contribution to the field of cybersecurity by providing a solution that not only protects users' digital identities but also upholds the fundamental right to privacy in the digital realm. With the ever-increasing value placed on personal data, the importance of such a system cannot be underestimated. The successful implementation of a zero-knowledge proof-based authentication system will represent a paradigm shift in how we approach security and privacy in an interconnected world.

2 BACKGROUND AND RELATED WORK

To provide context for the pressing need to enhance digital security mechanisms, this section delves into the prevailing protocols for user authentication and their associated challenges. We will explore the conventional triad of authentication factors, their vulnerabilities, and the consequent risks they pose to individual privacy and data security.

2.1 The Current State of Authentication

Authentication is the front line of defense in securing access to digital services. Current methods of authentication fall into three broad categories, often referred to as the factors of authentication: something you know (like a password), something you have (like a security token or smartphone), and something you are (like a fingerprint or other biometric data) [7]. While these methods have been effective to varying degrees, they come with inherent privacy and security challenges.

- **Passwords** are easily compromised through phishing, social engineering, or brute force attacks.
- **Security tokens** and **SMS-based two-factor authentication** can be intercepted or redirected by sophisticated attackers.

- **Biometrics**, although unique, pose serious privacy risks; once compromised, you cannot change your biometric data as you would a password.

These conventional methods often necessitate the storage of Personally Identifiable Information (PII) or sensitive data by the service provider, creating a potential target for attackers to exploit. Additionally, they depend on trusting a third party to securely handle data, a historical weak point that has led to significant vulnerabilities and breaches. [5]

2.2 Zero-Knowledge Proofs (ZKPs) in Authentication

Zero-knowledge proofs [6], introduced by Goldwasser, Micali, and Rackoff in the 1980s, provide a method for one party to prove to another that a statement is true without revealing anything beyond the validity of the statement itself. This cryptographic technique has the potential to revolutionize privacy in digital authentication.

Recent advancements have led to the great development of zk-SNARKs [4, 10] and zk-STARKs [1, 2], which facilitate non-interactive proofs that are succinct and quickly verifiable. These have seen practical application in blockchain technologies but are yet to be widely adopted in broader authentication systems due to their complexity and computational intensity.

Privacy-preserving authentication systems aim to verify users' credentials without exposing or storing any PII. Few existing systems, such as Idemix [3] and U-Prove [8, 9], allow for the selective disclosure of attributes, but they have not achieved mainstream use. The challenge is to create a system that is as user-friendly and quick as conventional methods while providing greater privacy and security.

2.3 Research Gap and Project Objectives

While ZKPs offer a theoretical basis for privacy-preserving authentication, there is a gap in practical, user-friendly applications that can operate at scale. The complexity of ZKP implementation, computational overhead, and lack of user-centered design are significant barriers.

A major challenge in the application of ZKPs to authentication is the computational overhead. Early ZKP systems required significant processing power, making them impractical for everyday use. Improvements in efficiency, particularly through the use of zk-SNARKs and zk-STARKs, have reduced these costs, but further optimization is needed for widespread adoption.

Another gap is the user experience. Authentication systems must be simple and intuitive to ensure user acceptance. Many ZKP-based systems are not designed with the average user in mind, leading to a lack of adoption despite their technical merits.

Finally, scalability and security are ongoing concerns. A practical ZKP-based authentication system must handle a large number of requests without compromising speed or security. Additionally, it must be robust against evolving cybersecurity threats.

3 EVALUATION PLAN

To rigorously assess the proposed system, we will employ a multi-dimensional evaluation plan encompassing qualitative and quantitative metrics.

3.1 Evaluation Metrics

- **Authentication Success Rate (ASR)**: The ratio of successful authentications to the total authentication attempts.
- **Authentication Time**: Duration from the initiation to completion of the authentication process.
- **System Efficiency**: Computational and memory resources utilized during authentication.
- **Security Analysis**: System robustness against common attack vectors.
- **User Satisfaction**: User experience assessed through surveys and interviews.
- **Scalability**: The system's ability to handle increased load effectively.

3.2 Data Collection

Data will be collected through system logs, user feedback, and security incident reports to provide a comprehensive evaluation of the system's performance.

3.3 Evaluation Methodology

A multi-stage evaluation approach, including laboratory testing, field testing, A/B testing, security auditing, and scalability testing, will be utilized to ensure a thorough assessment.

4 MILESTONE

The project will follow a series of milestones to ensure structured progress towards the system's development and evaluation.

4.1 Milestone 1: System Design and Initial Development

- Deadline: 2024-03-04
- Goals:
  - Complete a detailed literature review.
  - Finalize the system architecture.
  - Begin development of the authentication prototype.

4.2 Milestone 2: Prototype Testing and Iteration

- Deadline: 2024-04-05
- Goals:
  - Complete the prototype development.
  - Conduct initial internal testing and debugging.
  - Gather early feedback and iterate on the prototype.

4.3 Milestone 3: System Evaluation and Finalization

- Deadline: 2024-04-24
- Goals:
  - Perform comprehensive system testing, including security and performance evaluations.
  - Finalize the user interface based on usability testing feedback.
  - Prepare the project report and documentation.

REFERENCES

[1] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2018. Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive, Paper 2018/046. (2018). https://eprint.iacr.org/2018/046 https://eprint.iacr.org/2018/046.

[2] Aleksander Berentsen, Jeremias Lenzi, and Remo Nyffenegger. 2022. A Walk-through of a Simple Zk-STARK Proof. (December 2022). https://doi.org/10.2139/ssrn.4308637

[3] Jan Camenisch and Els Van Herreweghen. 2002. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*. Association for Computing Machinery, New York, NY, USA, 21–30. https://doi.org/10.1145/586110.586114

[4] Thomas Chen, Hui Lu, Teeramet Kunpittaya, and Alan Luo. 2023. A Review of zk-SNARKs. (2023). arXiv:cs.CR/2202.06877

[5] Aaron Fleury-Charles, Md Minhaz Chowdhury, and Nafiz Rifat. 2022. Data Breaches: Vulnerable Privacy. In *2022 IEEE International Conference on Electro Information Technology (eIT)*. 538–543. https://doi.org/10.1109/eIT53891.2022.9814044

[6] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. 1989. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* 18, 1 (1989), 186–208. https://doi.org/10.1137/0218012 arXiv:https://doi.org/10.1137/0218012

[7] Joseph Migga Kizza. 2024. *Authentication*. Springer International Publishing, Cham, 215–238. https://doi.org/10.1007/978-3-031-47549-8_10

[8] Christian Paquin. 2011. U-prove technology overview v1. 1. *Microsoft Corporation Draft Revision* 1 (2011).

[9] Christian Paquin and Greg Zaverucha. 2011. U-prove cryptographic specification v1. 1. *Technical Report, Microsoft Corporation* (2011).

[10] Maksym Petkus. 2019. Why and How zk-SNARK Works. (2019). arXiv:cs.CR/1906.07221

[11] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Jean-Jacques Schwartzmann. 2013. A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences* 7, 5 (March 2013), 95–107. https://hal.science/hal-00912435

[12] Xuerui Wang, Zheng Yan, Rui Zhang, and Peng Zhang. 2021. Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications* 188 (2021), 103080. https://doi.org/10.1016/j.jnca.2021.103080