Undergrad thesis summary

Jakob Povšič

2021

1 Introduction

The Internet has radically changed our society in the last decades, and every day our life is more digital. However not all changes are positive, today privacy seems like a necessary sacrifice in our digital lives, and it's becoming a more important issue because of the business models of big-tech companies that are based on accessing our data.

Zero-knowledge proofs (ZKPs) are one of the tools that could change our approach to working personal data. Their applications enable making decisions over data without disclosing the data itself.

In the thesis, we will explore the use of ZKPs in an authentication system, as a method of proving password correctness.

2 Authentication and the Extensible Authentication Protocol

Authentication is the process of verifying a claim an entity is making about itself or a subject. In information security authentication is commonly used for establishing access between users and protected system resources. Authentication with a username and password is a common model that everyone encounters daily.

In the thesis, we will design an authentication system as a method in the *Extensible Authentication Protocol* (EAP). EAP [1] is an extensible protocol for negotiation and execution of a variety of authentication methods (EAP methods). Our system will support authentication with a username and password over the network and will use a ZKP protocol as a mechanism for checking the password.

Password authentication has vulnerabilities, for which the industry has adopted security methods that prevent their exploitation. One of these methods is key-stretching, our authentication system has to use these tools to ensure a sufficient level of security.

3 Zero-Knowledge Proofs

Zero-Knowledge Proofs [3] are an interesting concept from the field of cryptography, that enable proofs of mathematical statements without revealing why they are true. This enables very interesting applications, where a system can operate with data without accessing them in their raw form. In such a system we can prove that we are of legal age or possess valid documents or that we have a sufficient bank account balance without revealing any sensitive information. Cryptocurrencies like Monero and Zcash are using ZKPs to validate transactions without revealing the identity of the sender, recipient, or the sum sent. Projects like Idemix [2], use ZKPs to achieve privacy-preserving verifiable credentials.

ZKP protocols are based on a certain class of mathematical problems. In our authentication system, we will use the ZKP protocol based on the quadratic residuosity problem.

4 Design of the authentication system as an EAP method

Our authentication system extends the ZKP protocol based on the quadratic residuosity problem, with key-stretching methods, which prevents offline attacks over data used for password verification. The authentication system is defined as an EAP method.

References

[1] Bernard Aboba, Larry Blunk, John Vollbrecht, James Carlson, Henrik Levkowetz, et al. Extensible authentication protocol. *RFC3748*, 2004.

[2] Jan Camenisch and Els Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 21--30, 2002.

[3] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186--208, 1989.