PAKE protocols and Decoy passwords

Sunday 7$^{\text{th}}$ January, 2024 - 12:04

Steve Meireles Lopes
University of Luxembourg
Email: steve.meireles.001@student.uni.lu

This report has been produced under the supervision of:
Marjan Skrobot
University of Luxembourg

Abstract—

Index Terms—

1. Introduction

1.1. Overview

Since the invention of personal computers, a username and password combination has been one of the most used authentication methods until today. Even though it is known that it has various drawbacks and weaknesses; including, humans being bad at making up strong and unpredictable passwords which makes it vulnerable to brute force and dictionary attacks. A problem a system administrator also has to solve is how to store the usernames and passwords. This is usually done in a password file (Example Linux: /etc/shadow /etc/passwd). In the past enterprises struggled with data breaches being open without them realizing or realizing too late, which resulted in leakage of their password files. This can be devastating to them and their clients. To make a system more secure one can incorporate fake accounts in the password file, therefore if somebody tries to enter the system using a fake account, the system administrator will be alarmed and know that the password file is in possession of outsiders. This report will analyze several security mechanisms one of them being fake passwords also called honeywords proposed by Juels and Rivest [1].

Although weak passwords are not secure they have some benefits, one of them is being very user-friendly and easy to remember. Nowadays, several protocols make it possible to securely authenticate peers by agreeing on a session key using a weak password. Such protocols are called PAKE protocols [2][3][4]. This report is going to analyze the PAPKE protocol of Bradley, Gamenisch, Jarecki, Lehmann, Neven, and Xu [5] in detail, which is a PAKE protocol using a public key. This protocol enables the ability to authenticate for example a browser without needing to trust a third party by using certificates, which is vulnerable to phishing attacks where attackers can pretend to be the authentication server.

The paper SweetPAKE of Skrobot and ... (need to ask the Tutor the name) [6] shows several approaches to combine both principles Honeywords and PAKE. They highlight the secure approaches and implementation. This report revolves mainly around the SweetPAKE paper, it analyzes the different approaches and offers an implementation of one approach. The implementation uses parts of code of the SPAKE2 implementation of warner [7].

Analyzing Honeywords, PAKE protocols, and SweetPAKE, this report tries to answer the question: How to detect if a password file is in possession of intruders and at the same time prevent phishing attacks?

1.2. Related Work

2. Honeywords

3. PAKE protocols

3.1. EKE

3.2. PAPKE

4. SweetPAKE

5. Application

5.1. Design

5.2. Implementation

6. Conclusion

7. References

References

[1] A. Juels and R. L. Rivest, "Honeywords: Making password-cracking detectable," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 145–160.

[2] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in International conference on the theory and applications of cryptographic techniques, Springer, 2000, pp. 139–155.

[3] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-authenticated key exchange using diffie-hellman," in Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19, Springer, 2000, pp. 156–171.

[4] R. Canetti, S. Halevi, J. Katz, Y. Lindell, and P. MacKenzie, "Universally composable password-based key exchange," in Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24, Springer, 2005, pp. 404–421.

[5] T. Bradley, J. Camenisch, S. Jarecki, A. Lehmann, G. Neven, and J. Xu, "Password-authenticated public-key encryption," in Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17, Springer, 2019, pp. 442–462.

[6] M. Skrobot, "Sweetpake: Key exchange with decoy passwords," in SweetPAKE, 2023.

[7] Warner, Python-spake2, https://github.com/warner/python-spake2, 2016.

8. Appendix