Combining Password Security with PAKE

Tuesday 24th October, 2023 - 17:13

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

This report has been produced under the supervision of:
Skrobot Marjan
University of Luxembourg
Email: marjan.skrobot@uni.lu

Abstract—In today's world, password security is very important. Most people have weak passwords which exposes them to brute force attacks. Furthermore malicious attackers also often use phishing attacks. These attacks expose a huge vulnerability and therefore a risk for the data of a lot of people. This project is to answer the scientific question: In the context of client-to-server authentication over an insecure network, how does one detect if a password file on the server side (containing usernames and passwords) was compromised by intruders and at the same time prevent phishing attacks on clients?

1. Main required competencies

1.1. Scientific main required competencies

For the scientific deliverable the needs to know the basics of cryptography and security such as password security, symmetric and assymetric encryption and key exchange. In addition to that he requires math knowledge such as set theory and math notations.

1.2. Technical main required competencies

The technical deliverable requires the student to know the same topics as for the scientifc deliverable. Moreover he will have to be able to program in the programming language python.

2. A Scientific Deliverable 1

A lot of enterprises use username and password logins to authenticate their users or employees. Everybody has a few technologies that require them to authenticate with their username and password. It is commonly known that this is often exploited by attackers through weak passwords, brute forcing or even pishing attacks. This brings us to the scientific question: In the context of client-to-server authentication over an insecure network, how does one detect if a password file on the server side (containing usernames and passwords) was compromised by intruders and at the same time prevent phishing attacks on clients?

To answer this question the deliverable will study password security, secure storage of password and brute forcing attacks. It will also study the honeyword paper from Riverst Juels [2] to find technologies to enhance the security propereties. Furthermore, it looks into ways to enhance current password authentication protocols from sending a hash of a user's password over TLS to utilzing PAKE which prevents pishing attack. On top of all that the paper is going to examine the SweetPAKE protocol from Arriage, Ryan and Skrobot [1] which uses the PAKE and enhances it with decoy password which adds password file leakage deetection mechanism at the server side.

3. A Technical Deliverable 1

The technical deliverable will be an implementation of a decoy password generator according to proposed protocols from the Honeyword paper [2] of Riverst Jules and the SweetPAKE protocol [1] suggested from Arriaga, Ryan and Skrobot in the programming language python.

This project is beneficial to the security world considering there are not a lot of open-source PAKE implementations despite of its security value. Combining PAKE with a decoy password generator which further enhances password security does not exist in the current market.

The program will contain a password file which simulates a password file in the real world. It needs to have the ability to generate decoy passwords in a way that an intruder cannot guess the correct password. It will have an index file which simulates a file that an extern server, named here the honeychecker, would have. The program should be able to check if the password given by the user is the correct one. The program should

also use SweetPake protocol to communicate between server and client.

To be able to achieve this program will use the open-source project python-spake2 of warner as reference. It will use the standard library random and hashlib to encrypt and generate passwords.

References

[1] Ryan Arriage and Skrobot. “SweetPAKE: Key exchange with decoy passwords”. 2023.

[2] Ari Juels and Ronald L Rivest. “Honeywords: Making password-cracking detectable”. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. 2013, pp. 145–160.