Hacettepe University

Computer Engineering Department

BBM465 Information Security Lab. - 2024 Fall

Assignment 3

November 27, 2024

2220356141 - Ayşe Yaren Topgün

2210356008 - Sûdenaz Yazıcı

Introduction

In this project, we developed simple user portal which user can register and login. We mostly focused on security when managing and storing user information using text-based database and hash chain-based OTP authentication step. We have two sides including Client side and Server side.

Part 1: User Registration

In registration part, user enters a username and password. Client side checks specified conditions(The username should not include any special characters and numbers. A password should be larger than 6 characters.) and if not satisfied, it does not save to database and shows the necessary warning messages. If the conditions satisfied, the password is hashed by SHA-256 and username, hashed password and the OTP token achieved by hashing the password counter(100) times are sent to Server side. Server side takes this information and after decrypting the already existing database, it saves the new information to database. After saving, Server encrypts the database again and updates the text in database file.

Part 2: User Database

As explained in the section above, the entire database is encrypted (by the RSA algorithm) for information security. For each user, an username, a hashed password and OTP token are stored. The structured format is like this ” username1;hashedpassword;OTPToken;Counter\nusername2;hashedpassword;OTPToken;Counter…”.

Part 3: User Login

In login part, user enters username and password. This information sent to Server side to check if given user exists. After checking the credentials, OTP token is created but this time the password is hashed 1 time less than before. This information is sent to Server side. There is already stored OTP token for user in database so, the Server firstly hashes the token received from Client side one time and compares it to token in the database. If they match, the login process is confirmed.

References

[1] https://flask.palletsprojects.com/en/stable/

[2] https://pycryptodome.readthedocs.io/en/stable/

[3] https://pycryptodome.readthedocs.io/en/latest/src/cipher/oaep.html