CIS 446 Term Project Report

Title: SECURE MOBILE MESSAGING APP

Author: Ali Ramadan

Course: CIS 446 – Wireless and Mobile Computer Security

Instructor: Dr. John P. Baugh

Date: April 2025

1. Introduction

This project presents a socket-based chat application with end-to-end encryption implemented in Python. The application uses the Fernet symmetric encryption scheme to secure communication between a client and a server across a network. It demonstrates how encrypted messaging can be implemented using low-level networking tools in a secure and practical way.

2. Project Description

The system consists of two Python scripts:

1. Server Script (secure\_chat\_server.py)
   * Listens for client connections on a specified port.
   * Decrypts incoming encrypted messages and displays them.
   * Accepts input from the server user, encrypts it, and sends it back to the client.
2. Client Script (secure\_chat\_client.py)
   * Connects to the server using its IP address and port.
   * Sends encrypted messages to the server.
   * Receives and decrypts the encrypted responses.

Messages are encrypted before transmission and decrypted upon receipt, ensuring that plaintext messages never leave the local machine.

3. Tools and Technologies

* Python 3.10
* cryptography (Fernet module) for AES-based encryption
* socket for network communication

4. Implementation Details

Encryption Key: A 32-byte Fernet key is generated once and shared securely between the client and server. This key is essential for both encrypting and decrypting messages.

Chat Logic:

* Users input messages in their respective terminal windows.
* Messages are encrypted using Fernet before being sent.
* Incoming encrypted messages are printed alongside their decrypted form.
* Chat ends when either user types exit, and the socket connection is closed cleanly.

5. Security Considerations

* All messages are encrypted before transmission and decrypted only on the receiving end.
* The encryption key is shared in advance and kept private, or can be generated individually
* Fernet provides built-in message integrity verification to prevent tampering.
* Errors during decryption are handled gracefully to avoid crashes.

6. Limitations and Future Work

* The encryption key must be manually shared between users.
* The system lacks authentication mechanisms or encryption key negotiation.
* Future versions could use RSA to securely exchange the Fernet key or integrate a GUI for ease of use.

7. Conclusion

This project demonstrates a practical and educational implementation of secure, encrypted chat over a network using sockets. It aligns with course objectives by showcasing encryption in action within a mobile/wireless security context. The program is simple, effective, and highlights the value of securing communication at the transport level.

Thank you for reviewing my project.