CSC380 Computer Security Project - Spring 2024
Secure Chat Part 2

Prof. William Skeith
Dahyeon Park, Jiazhou Zhang
May 19th, 2024

1. **Assumptions**

   We assume that the communicating parties have already exchanged their public keys securely through an out-of-band mechanism. This means that before initiating any communication using the chat program, users must have a trusted method of sharing their public keys with each other to avoid the complexities and potential vulnerabilities associated with a public key infrastructure (PKI). The system also assumes that each party's private keys and any derived session keys are securely stored and managed, preventing unauthorized access or leakage. Furthermore, it is assumed that the adversary has significant capabilities, including intercepting, modifying, or replaying messages exchanged between the communicating parties (Man-in-the-Middle attacks). The adversary has access to the network and can perform active attacks, such as injecting messages or impersonating a participant. However, it is also assumed that the adversary cannot break the cryptographic primitives (AES-256, HMAC-SHA-256, Diffie-Hellman key exchange) within a feasible time frame using current computational resources. The security of the random number generator used by the cryptographic library (OpenSSL) is also assumed to be strong and unpredictable.

2. **Claims**

   a. **Integrity:** Each message includes a Message Authentication Code (MAC) generated using HMAC-SHA-256. This ensures that any modification to the message during transit will be detected by the recipient. The integrity

of the message is verified before decryption, preventing attacks that modify the ciphertext to induce predictable changes in the plaintext.

b. **Confidentiality:** In our code, All messages exchanged between the communicating parties are encrypted using AES-256 in CBC mode. This ensures that an adversary who intercepts the messages cannot read their contents. Session keys derived from the Diffie-Hellman key exchange are used for encryption. These keys provide perfect forward secrecy, meaning that if a session key is compromised, it does not affect the security of past sessions.

c. **Mutual Authentication:** Both communicating parties authenticate each other using their respective public keys. This prevents an adversary from impersonating one of the parties. The Diffie-Hellman key exchange ensures that both parties agree on a shared secret, which is used to derive session keys for encryption and MAC generation. This mutual agreement ensures that both parties are legitimate and in possession of their private keys.

d. In the case of malicious communicating party:
As mentioned above, in the case of a malicious communication party performing Man-in-the-Middle attacks, they can decrypt, read, and modify messages. Hence, it would be good to integrate such as certificate verification to ensure the authenticity of public keys exchanged.