CSC380-Project-Secure-Chat

Team Member: Zhi Gao, Wendian Jiang, Xinwei Wu

Assumptions:

-Secure Operating Environment: We assume that the participating users are using secure devices and operating systems that are not compromised by malware or other malicious software.

-Secure Communication Channels: We assume the underlying communication channels used by the chat program are secure, utilizing TCP/IP communication mechanisms.

-Authentication: We assume that the communicating parties are authenticated by a valid three-handshake protocol. It can correctly identify whether the other party is an attacker or a normal user.

-Public Key Infrastructure (PKI): We assume that each communicating party already possesses the public key of the other party. This implies that the public key exchange has already taken place through a trusted and secure mechanism.

-Strong Encryption: We assume that a strong encryption algorithm is used. AES (Advanced Encryption Standard) has a long enough key length to protect the confidentiality of the message.

Attacker Resources:

-Eavesdropping: We assume that attackers have the capability to intercept and capture network traffic between the communicating parties.

-Message Tampering: Attackers can modify the content of messages sent between the communicating parties.

-Spoofing: Attackers can impersonate one or both of the communicating parties and attempt to deceive the other party.

-Denial of Service (DoS): Attackers may try to disrupt or prevent communication between the parties by overwhelming the chat program's resources or network infrastructure.

-Cryptanalysis: Attackers may attempt to break the encryption algorithms or exploit any weaknesses in the implementation to gain unauthorized access to message content.

Claims:

-Mutual Authentication: Before the chat begins, both parties will perform a three-way handshake. This means that each party can verify the identity of the other party and confirm their authenticity, providing assurance that the communication is taking place with the intended recipient.

-Integrity: The chat program ensures the integrity of messages by employing message authentication codes (MAC). This mechanism allows the recipient to verify that the received message has not been tampered with during transit.

-Confidentiality: The chat program guarantees the confidentiality of messages through the use of strong encryption algorithms. The content of messages remains encrypted during transmission and can only be decrypted by the intended recipient with the corresponding shared key.

-Protection against Malicious Parties: The chat program considers the worst-case scenario where a communicating party is malicious or running a modified, evil version of the program. In this case, the chat program's design incorporates measures to detect and handle malicious behavior. If such behavior is detected, the program may terminate the session or prompt the user with a warning.