Security Overview of Secure Chat

Assumptions

- **Secure Environment:** It is assumed that the operating environment is secure, and the underlying hardware and OS are not compromised.
- **Trustworthy Certificate Authority (CA):** The SSL certificates used are assumed to be issued by a trusted CA, and the certificate verification process during SSL handshake ensures authenticity.
- **Reliable Cryptographic Libraries:** The OpenSSL library used in the application is assumed to be up-to-date and free from vulnerabilities at the time of deployment.
- **Informed Users:** Users are assumed to be aware of basic security practices, such as keeping their private keys secure and verifying the identity of the server and client during connections.

Claims

- **Confidentiality**: All messages exchanged between the client and server are encrypted using SSL/TLS, ensuring that eavesdroppers cannot read the content of the messages.
- **Authentication:** Both the server and client use certificates for SSL/TLS handshakes, which authenticate the identities of the parties involved in the communication.
- **Integrity:** SSL/TLS also ensures the integrity of the transmitted data, protecting against alterations during transit.

Limitations

- **Endpoint Security:** The application does not directly address endpoint security; if the client or server systems are compromised, the security of the entire communication channel could be jeopardized.

- **Certificate Management:** Mismanagement of certificates, such as failure to revoke certificates of compromised systems, can lead to vulnerabilities.
- **Physical Security:** The application assumes the physical security of the hosting servers and client machines, which if compromised, can lead to unauthorized access.
- **Forward Secrecy:** The code does not explicitly ensure forward secrecy, which would protect past sessions against future private key compromises.
- **Denial of Service (DoS):** The application does not include mechanisms to protect against DoS attacks, which could make the service unavailable to legitimate users.