Peer Review Report for Group 7 – Md Raiyan Rahman

Vulnerabilities

- **Backdoor 1 - Lack of Input Validation**: When reading from the clients.txt file, server.cpp does not validate the input. An attacker could use this file to introduce malicious data into the system, perhaps resulting in buffer overflows or command injection attacks.

- **Backdoor 2 - Insecure Key Management**: The RSA keys generated and saved by the encrypt.cpp function are stored in files (PEM_write_RSA_PUBKEY and PEM_write_RSAPrivateKey). However, there is no inquiry of how to protect or manage these key files.

```
11
12  void save_rsa_public_key(RSA* rsa, const char* filename) {
13      FILE* fp = fopen(filename, "w");
14      PEM_write_RSA_PUBKEY(fp, rsa);
15      fclose(fp);
```

Strengths:

- The use of AES-GCM encryption protects data confidentiality and integrity, which is a good practice for securing communications.

- For cryptographic activities, the code makes use of existing libraries such as OpenSSL. Using trusted libraries helps to avoid various security issues that can arise when implementing encryption algorithms yourself.

Weaknesses:

- There is no error handling for encryption and decryption failures.

- The RSA private key is kept in a file called encrypt.cpp without any specific security measures. The file is saved to the disk without encryption, which means that if an attacker gains access to the machine, they could potentially obtain the private key, jeopardizing the security of all encrypted conversations.

Recommendations

- To appropriately manage failures, introduce error handling into cryptographic functions. For example, if an encryption or decryption operation fails, note the problem and respond appropriately (retry, notify the user).

- Ensure that all data read from external sources (such as clients.txt) or user input is verified and sanitized before processing. This involves checking IP addresses, message formats, and command structures to prevent injection and overflow threats.

Thanks for the work hard on the chat application, the function is work pretty good.