HW #3

Secure Chat Program

Computer Security

School of CSEE

Requirement

- 본 숙제는 OpenSSL을 활용하여 Multi-thread 및 TLS 기반의 Secure Chat Program을 개발하는 것 입니다.

- 서버와 클라이언트 모두 개발해야 합니다.

- 제공하는 chat_serv.c 와 chat_clnt.c 를 참고하세요.

- 서버와 클라이언트는 OpenSSL을 사용하며, TLS Handshake 이후 주고 받는 데이터는 모두 암호화 되어야 합니다.

Requirement

- 클라이언트는 다른 클라이언트와 메시지를 주고 받을 수 있을 뿐만 아니라 대화 도중 파일도 공유할 수 있습니다.

- 파일을 공유하고자 하는 클라이언트는 메시지 입력 부분에서 아래와 같이 “file_share: hgu.jpg” 를 입력하면 hgu.jpg를 암호화하여 서버로 전송합니다. 이 경우 “file_share:” 는 클라이언트에게 보내는 메시지가 아니라 Command로 인식됩니다.
  - 예: Type message> file_share: hgu.jpg

- 서버로 전송된 파일은 서버를 경유하여 나머지 모든 클라이언트들에게 전송됩니다.

Requirement

- 프로그램 언어는 C 언어를 사용하세요.
- 기타 언급 되지 않은 사항 (입출력 형식, Command, Ciper spec, Certificate 등) 은 나름대로 설정하여 구현하시면 됩니다.
- 입출력 형식은 자유롭게 하되 가독성 있게 구현하세요.
- 구현된 코드는 make 명령어를 통해 컴파일 되어야 합니다.
- Intel CPU 사용자의 경우 Seed VM에서 실행되어야 하며, Arm CPU 사용자는 Arm 버전 Ubuntu 22.04에서 실행 가능해야 합니다.

Requirement

- 코드 내에서 OpenSSL에서 제공하는 함수를 사용할 경우 해당 함수가 무엇을 위해 사용하는 함수인지 주석을 추가하세요.

- OpenSSL 사용을 위해 ChatGPT와 같은 AI Tool이나 다양한 오픈소스의 도움을 받을 수는 있으나 코드를 그대로 복사하면 안됩니다.

- 다른 학생들과 구현 방법에 대한 Discussion은 얼마든지 가능하나 코드 공유는 불가합니다.

Requirement

- 제출 폴더 안에는 다음과 같은 것들이 포함되어야 합니다.
  - 서버: tls_chat_serv.c
  - 클라이언트: tls_chat_clnt.c
  - 프로그램 실행에 필요한 각종 C 파일 또는 Header 파일
  - 프로그램 실행에 필요한 Private Key, Certificate 파일
  - Makefile: tls_chat_serv.c 와 tls_chat_clnt.c 가 모두 컴파일 되어야 함.
  - README.txt: 구현한 프로그램의 사용 방법(서버/클라이언트 모두), 사용 라이브러리 버전 등 프로그램 컴파일과 실행에 필요한 모든 정보
  - Screenshot.pdf: 실행 화면을 스크린 캡처한 파일 (서버/클라이언트 모두)

- 제출하는 파일들은 아래와 같은 형태로 ZIP으로 압축하여 LMS에 제출하세요.
  - 파일 이름: hw03_student id.zip (ex: hw03_20400022.zip)

- Due date: 11:59pm, 12/12 (Thu)