정보보호론\_기말고사

12141163 이욱진

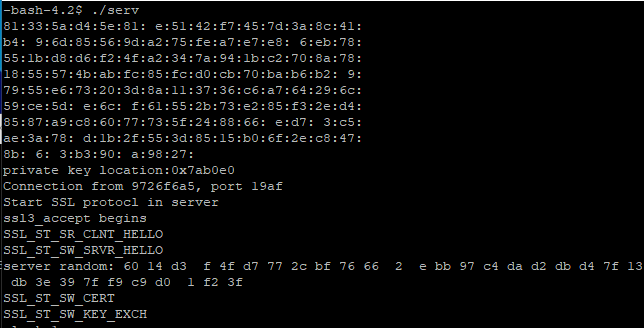
2020.12.11(금)

(1) Modify openssl such that the random numbers included in the ServerHello message are displayed during the client and server communication. **You have to explain in detail how you have solved this problem.**

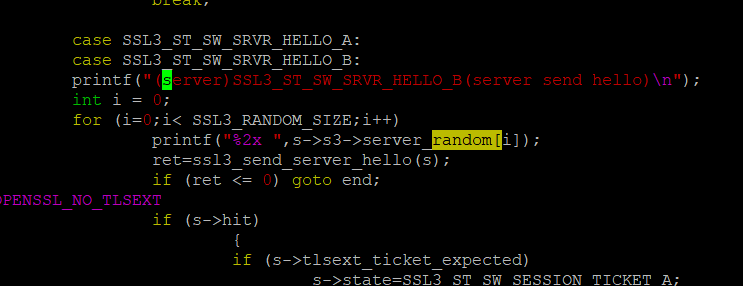
client:

..........................

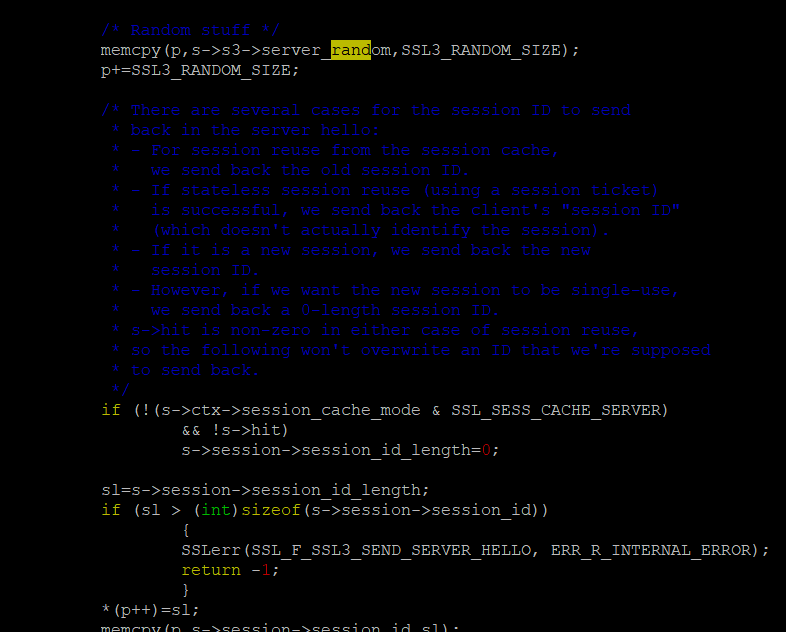
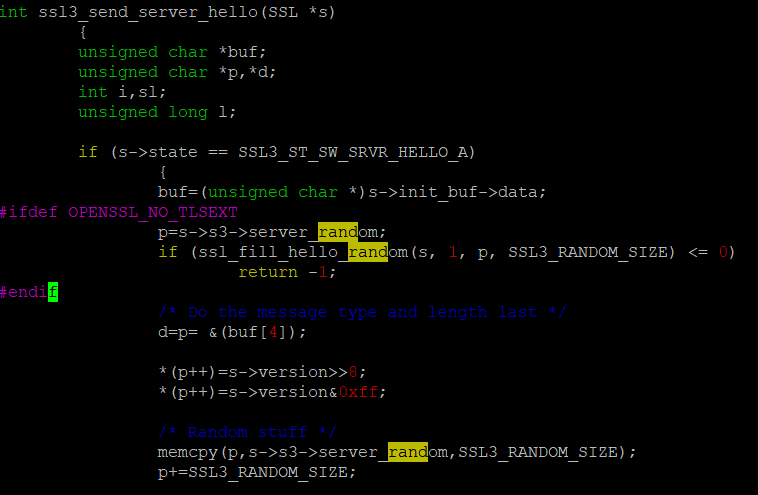
server:



우선 openssl에 s3\_srvr.c 파일을 찾아보았고 accept부분 내부에 서버가 클라이언트에게 hello를 보내는 부분(ssl3\_send\_server\_hello 함수 호출하는 부분)을 찾았습니다.



그리고 더불어 serverhello에 포함이되는 random number를 rand 키워드를 통하여 알아보았습니다.



Server hello의 구조를 일단 살펴보면

server -> client: server hello

protocol version (TLSv1)

session ID

chosen cipher suite

key exchange algorithm (RSA)

symmetric key algorithm (DES)

message digest algorithm (SHA-1)

compression algorithm (PKZip)

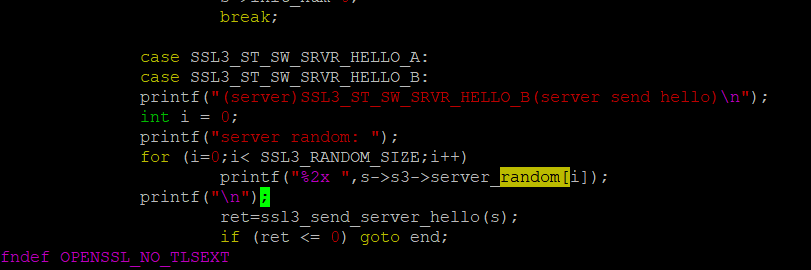
random number (823, 495, 127)

다음과 같습니다.



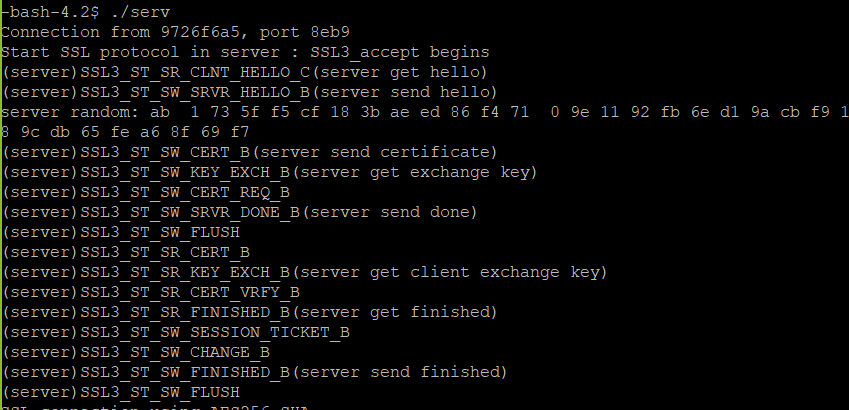
<기존 과제에서 스니퍼를 활용하여 hello 정보를 출력해보았던 사진>

다음과 같습니다. 그리고 그 중에서 위 2번째 사진 속 내용을 살펴보면 sessionID len을 출력하기 전에 random number를 출력하게 되었는데 이는 기존 과제에서도 다룬 스니퍼를 활용하여 데이터를 살펴보았을 때와 순서가 같았습니다. 그래서 아래 사진과 같이 ssl3\_send\_server\_hello 함수를 호출하기 전 random number를 출력하게 해주었습니다.



Make, make install을 한 후에 이어서 g++로 serv, cli를 다시 컴파일해주고 다음과 같은 결과를 확인할 수 있었습니다.

./serv



Random number는 32bit형식을 가지는데 출력된 결과 역시 32비트가 출력되었음을 알 수 있었습니다.

./cli

