컴퓨터공학 All in One

C/C++ 문법, 자료구조 및 심화 프로젝트 (나동빈)
제 71강 - 공개키 기반 구조

공개키 기반 구조

패킷 도청

SSL(Secure Sockets Layer)은 서버와 클라이언트 간의 패킷을 암호화하기 위한 프로토콜입니다.

암호화를 거치지 않게 되면 서버와 클라이언트 중간에 있는 공격자가 패킷 도청을 통해서 패킷의 내용을 확인하여 공격을 수행할 수 있습니다. 따라서 SSL을 이용하여 다양한 프로그램 환경에서의 패킷을 암호화해야 합니다.

공개키 기반 구조

대칭키 암호화

대칭키 암호화 방식은 서버와 클라이언트가 하나의 키(Key)를 가지고 통신하는 방식입니다. 대칭키 암호화 방식은 속도가 빠르다는 장점이 있으나 키(Key) 값이 노출되는 경우 보안이 취약하다는 단점이 있습니다.

공개키 기반 구조

공개키 암호화

공개키 암호화 방식은 공개키(Public Key)와 개인키(Private Key)가 사용되는 방식입니다. 서버는 공개키를 모두에게 공개한 뒤에, 각 클라이언트는 그 공개키를 이용해 데이터를 암호화하여 서버에게 전송합니다.

공개키로 암호화된 데이터는 오직 서버의 개인키를 이용해서만 해독할 수 있으므로, 클라이언트에서 서버로 가는 데이터를 중간에서 변조할 수 없습니다.

공개키 기반 구조

인증서

인증서(Certificate)란 공개키와 개인키에 대한 정보를 포함하는 인증 도구입니다. 정부기관 등의 공인된 기관에서 인증을 통해 발급받을 수 있으며, 본인이 직접 사설 인증서를 만들 수도 있습니다.

공개키 기반 구조

SSL 통신 과정

일반적으로 SSL을 이용하는 통신 과정은 다음과 같습니다.

1. 서버가 클라이언트에게 공개키 정보가 담긴 인증서를 보냅니다.
2. 클라이언트는 서버로부터 받은 인증서를 통해 신뢰성을 검증할 수 있습니다.
3. 클라이언트는 대칭키를 생성하여 공개키로 암호화 한 뒤에 서버로 전송합니다.
4. 서버와 클라이언트는 해당 대칭키를 이용하여 통신합니다.

공개키 기반 구조