1. HTTP는 TCP 80번 프로토콜으로

Hypertext형식의 문서(HTML) 문서를 인터넷에서 주고 받을 때 사용하는 프로토콜

평문전송이기에 이를 스니핑하여 악용할 수 있어 보안성이 많이 떨어진다.

2. HTTPS는 HTTP에 SSL/TLS를 적용한 프로토콜으로 HTTP보다 보안성이 뛰어나다.

로그인하는 경우나 대표적인 사이트에는 대부분 HTTPS를 사용한다.

S는 Over Secure Socket Layer의 줄인말이다

TLS를 사용하면 인증서를 사용하여 데이터를 암호화하고 데이터 전송 중 수정되거나 손상되는 것을 방지한다.

3. SSL/TLS

SSL과 TLS는 같은 것

SSL은 네스케이프가 만들었고 3.0까지 나왔다가 IETF가 표준화하여 만든 것이 TLS이다.

SSL 동작과정

SSL의 암호화에는 공개키와 대칭키를 함께 사용한다

실제 데이터의 전송에는 대칭키를 사용하고

대칭키 공유에는 공개키를 사용한다.

핸드셰이킹 – 세션 – 세션 종료 총 3가지 단계를 걸친다.

핸드셰이킹은 서로의 신원을 확인하고 Master Secret과 세션키를 생성하기 위해 한다.

핸드 셰이킹은 총 6가지 과정으로 이루어진다.

1. 클라이언트 -> 서버로 랜덤데이터를 전송하는 Client Hello

2. 서버 -> 클라이언트로 랜덤데이터를 전송하는 Server Hello

3. 클라이언트 측에서 인증서를 확인하고 Pre Master Secret을 생성

4. Pre Master Secret을 암호화 하고 서버 측으로 전송

5. Pre Master를 복호화 하고 세션키를 생성

6. 서버 측과 클라이언트 측이 Master Secret키와 Session 키를 생성

이제 Session 키를 사용하여 서로 통신, 이 과정이 세션 단계이고 종료된다