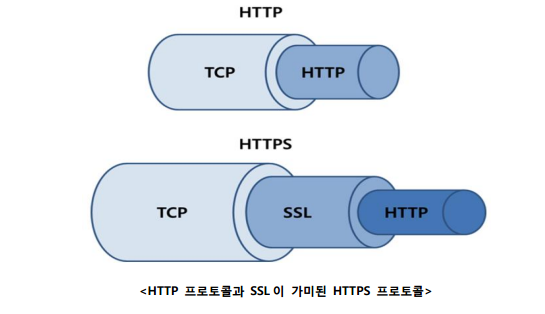
2017년 1학기 네트워크 기초 과제

**SSL / TLS 프로토콜**

게임공학과 2015182014 성예솔(목요일 10~12교시)

SSL(Secure Socket Layer) 은 인터넷을 이용한 정보 보안의 안전한 거래를 위해서 Netscape 회사에서 만든 인터넷 통신 규약 프로토콜이다. 이에 기초로 해서 IETF에서 SSL보다 안전하고 정확한 TSL(Transport Layer Security)을 만들었다. 전송계층에서 서버와 클라이언트를 상대로 인증과 암호화를 하는 보안용 프로토콜들이다. 응용계층과 전송계층 사이에서 안전한 보안채널을 형성해주는 역할을 한다.



TLS 1.2 버전은 만들어 진지 8년이 지났다. 8년동안 이 프로토콜의 결함이 드러나는 몇 가지 공격이 나온 뒤로 IETF는 새로운 프로토콜을 개발하였다. TLS 1.3은 최근에 인터넷 사용자를 위해서 속도와 보안이 향상된 새로운 암호화 프로토콜이다. 2016년 말에 완성되었고 1.2와 다른 점은 보안이 강화되었고 속도도 향상되었다. TLS1.3은 이전 버전의 프로토콜을 공격한 방법으로는 전혀 영향을 끼치지 못한다. 그리고 1.3 버전은 간소화되어 서버 운영자가 훨씬 간단하게 구성 할 수 있게 되었다. 그리고 훨씬 속도가 빨라져 더나은 웹 브라우징 환경을 제공한다.