* HTTP 와 HTTPS 는 무엇이며 그 차이는?

HTTP(HyperText Transfer Protocol)는 하이퍼텍스트를 빠르게 교환하기 위한 프로토콜의 일종이다. 80 번 포트를 사용한다. HTTP 는 서버와 클라이언트의 사이에서 어떻게 메시지를 교환할 지를 정해놓은 규칙인 것이다.HTTP 의 구조는 요청(Request)와 응답(Response)로 구성되어 있다.(하이퍼링크로 예를 들어보자, 클라이언트가 웹 페이지에서 링크가 걸려있는 텍스트를 클릭(요청)하면 링크를 타고 새로운 페이지로 넘어간다(응답))

*프로토콜
통신 프로토콜 또는 통신 규약은 컴퓨터나 원거리 통신 장비 사이에서 메시지를 주고 받는 양식과 규칙의 체계이다. 통신 프로토콜은 신호 체계, 인증, 그리고 오류 감지 및 수정 기능을 포함할 수 있다. 프로토콜은 형식, 의미론, 그리고 통신의 동기 과정 등을 정의하기는 하지만 구현되는 방법과는 독립적이다. 따라서 프로토콜은 하드웨어 또는 소프트웨어 그리고 때로는 모두를 사용하여 구현되기도 한다.

HTTPS(Hypertext Transfer Protocol over Secure Socket Layer)는 월드 와이드 웹 통신 프로토콜인 HTTP 의 보안이 강화된 버전이다. HTTPS 는 소켓 통신에서 일반 텍스트를 이용하는 대신에, TLS 프로토콜을 통해 세션 데이터를 암호화한다. 따라서 데이터의 적절한 보호를 보장한다. HTTPS 의 기본 TCP/IP 포트는 443 이다. 보호의 수준은 웹 브라우저에서의 구현 정확도와 서버 소프트웨어, 지원하는 암호화 알고리즘에 달려있다. HTTPS 를 사용하는 웹페이지의 URL 은 'http://'대신 'https://'로 시작한다.

TSL 기반의 https 가 보안에 안정성이 높은 이유는 해독키를 통신시 주고받는 http 와 달리 https 는 공개키만 통신시 전송하고 개인키는 통신시 이동하지 않는다. 암호 해독을 위해서는 공개키와 개인키를 모두 보유하여야 하는데 (공개키로 암호화한 문서는 개인키로만 해독이 가능하고 개인키로 암호화한 문서는 공개키로만 해석이 가능하기 때문) 개인키를 해커가 가로챌 방법이 없기 때문에 보안상 http 보다 우위를 점하고 있다.

*TLS
인터넷에서의 정보를 암호화해서 송수신하는 프로토콜. 넷스케이프 커뮤니케이션스사가 개발한 SSL(Secure Sockets Layer)에서 기반한 기술로, 국제 인터넷 표준화 기구에서 표준으로 인정받은 프로토콜이다. 표준에 명시된 정식 명칭은 TLS 지만 아직도 SSL 이라는 용어가 많이 사용되고 있다.

인터넷을 사용한 통신에서 보안을 확보하려면 두 통신 당사자가 서로가 신뢰할 수 있는 자임을 확인할 수 있어야 하며, 서로간의 통신 내용이 제 3 자에 의해 도청되는 것을 방지해야 한다. 따라서 서로 자신을 신뢰할 수 있음을 알리기 위해 전자 서명이 포함된 인증서를 사용하며, 도청을 방지하기 위해 통신 내용을 암호화한다. 이러한 통신 규약을 묶어 정리한 것이 바로 TLS. 주요 웹브라우저 주소창에 자물쇠 아이콘이 뜨는 것으로 TLS 의 적용 여부를 확인할 수 있다.

예를 들어 인터넷 뱅킹을 하기 위해 은행의 사이트에 방문했을 때, 고객은 그 사이트가 정말 은행의 사이트가 맞는지 아니면 해커가 만든 가짜 피싱 사이트인지 확인할 수 있어야 하며, 은행 역시 자신의 서비스에 접속한자가 해당 고객이 맞는지 아니면 고객의 컴퓨터와 서버 사이에서 내용을 가로채고자 하는 해커인지 확인할 수 있어야 한다. 그리고 은행과 고객 간의 통신 내용이 다른 해커에게 도청되지 않도록 내용을 숨겨야 한다. 이럴 때 바로 은행과 고객 간에 TLS 를 사용한 연결을 맺어 안전하게 통신을 할 수 있다. 구체적으로 서로의 신원을 확인하기 위해 핸드셰이크(Handshake) 과정을 거치며, 쉽게 요약해서, 먼저 서로가 어떤 TLS 버전을 사용 가능한지를 확인하고, 인증서를 사용해 서로를 믿을 수 있는지 확인한 뒤, 서로간의 통신에 쓸 암호를 교환하는 것이다. 그 다음부터는 서로 교환한 암호를 사용해 제 3 자가 도청할 수 없는 암호화된 통신을 하면 된다.

*국내 공인 인증서가 생긴 배경과 그 위험성은?

1. 공인인증서가 생긴 정치적 법률적인 배경
1999 년 전자서명법이 발효되면서 전자정부의 초석을 다지기 위해 11 명의 암호학 교수들이 모여서 연구를 시작했다. 그러나 연구 도중 두 파벌로 나뉘면서 상공회의소+행정부를 중심으로 한 축과 금융결제원, 은행, 보험등 금융업계로 나뉘게 된다. 이에 따라 전자는 모든 국민의 개인정보를 행정부가 보증하게 되었고, 입찰을 통해 사인 발급자로서 한국정보인증(KICA, Signgate)이 담당하게 되었다. 반면 후자는 금융결제원(yessign)이 발급 주체가 되었고, 은행, 보험회사들이 보증 주체가 되었다. 이는 전자인감이 필요한 공적 증명을 행정부가 맡고, 일반 은행 거래 정도는 금융결제원이 한다는 초기 목표가 있었기 때문에 이뤄진 것이다.

2. 공인인증서가 생긴 기술적인 배경과 위험성
TSL 기반의 암호화 기술 도입으로 국내에도 관련 암호화 시스템이 필요했고 이로 공인인증서의 필요성이 대두되었다. 하지만 미국정부가 40bit 짜리 공개키 기술만 수출할 수 있게 하다보니 보안수준이 충분치 않았고 국내에서는 KISA 가 독자적으로 SEED 라는 암호화 알고리즘을 만들다. 하지만 이것이 국제적인 표준이 되지 않다보니 IE 를 비롯한 브라우저 업체에서 여기에 대한 지원을 하지 않았고, 실제 브라우징에 암호화 방식을 적용하기 위해서 부득이하게 Active X 를 사용한 플러그인이

만들어 적용했다. SEED 를 사용하다보니 KISA 의 인증서는 국제적으로는 공인 인증서로 인정받지도 못하고 있는 상황이라고 하며, 대안으로 사용할 플러그인(Active x)는 iE 에서만 돌아가고 있으니 그 동안 파이어폭스나 크롬 같은 브라우저에서는 인터넷 뱅킹이나 전자 상거래를 사용할 수 없다.
실제 공인인증서의 베이스인 SEED 보안 알고리즘은 보안 안정성이 검증되어 공인인증서 자체의 안정성에는 문제가 없으나, 배포시 ActiveX 를 사용하기에 사용자에게 IE 환경을 강제하고 악성코드에 노출되게할 가능성이 높아진다. 신뢰할 수 있는 곳(예를 들면 은행 사이트나 정부 기관, 어도비 사)에서 나온 액티브 X 라면 악성 코드가 나올 가능성이 희박하나 문제는 제작자와 제작사가 불명이거나 신뢰할 만한 액티브 X 로 보이도록 가장한 것도 있다는 것이다. 습관적으로 설치를 누르는 행위는 악성코드 감염의 첫 걸음이다.

*위 내용을 조사하며 느낀점은?

어제부터 계속 ActiveX 의 폐해를 보니 지겹기도 하지만 그 만큼 보안이 통신에서 얼마나 중요한 부분인지 생각하게되었다. 특히 암호화에 대한 고민이 2 차 세계대전 이전부터 시작되었고, 이미 완성도 높은 기술도 그 당시 구현했다는 부분이 놀라운데 역시 기술은 전쟁으로 비약적인 발전을 하는구나 싶기도 하다.. 하나 의외인 부분은 그렇게 욕을 많이 먹은 공인인증서가 기술적으로 허접한 녀석은 아니었다는거? SEED 알고리즘은 완성도가 높았구나..
마지막으로 역시 기술을 선도해야 미국한테 장난질 안당하겠구나 싶다.