20160105 서은정
http와 https, 공인인증서

1. HTTP와 HTTPS

HTTP와 HTTPS 모두 Hypertext인 HTML을 전송하기 위한 통신규약을 의미한다. HTTPS의 마지막의 S는 Over Secure Socket Layer의 약자로 Secure라는 말을 통해서 알 수 있듯이 보안이 강화된 HTTP라는 것을 짐작할 수 있다. 여기서 말하는 '보안'이란 데이터를 암호화 한다는 의미이며 암호화 방식에는 SSL / TLS 이 있다.

- SSL 과 TLS

  둘 다 모두 네스케이프에 의해서 발명되었고 SSL이 표준화된 것이 TSL이므로 동일한 것이라고 할 수 있다.(표준화된 이름은 TSL이지만 SSL이란 이름이 훨씬 많이 사용되고 있다)

**데이터를 어떻게 암호화 하나?**

일단 서로 데이터를 주고받을 당사자들 서로가 신뢰할 수 있는 자임을 확인해야 한다.(hand shacke) 그 과정은

1. 먼저 클라이언트에서 서버에 ClientHello 메시지를 보낸다. 여기에는 클라이언트에서 가능한 TLS 버전, 세션 식별자, 암호 설정 등의 정보가 포함된다.

2. 클라이언트의 메시지를 받은 서버는 ServerHello 메시지를 클라이언트에게 보낸다. 여기에는 ClientHello 메시지의 정보 중 서버에서 사용하기로 선택한 TLS 버전, 세션 식별자, 암호 설정 등의 정보가 포함된다.

3. 서버가 클라이언트에 Certificate 메시지를 보낸다. 여기에는 서버의 인증서가 들어간다. 이 인증서는 별도의 인증 기관에서 발급받은 것이며, 서버가 신뢰할 수 있는 자임을 인증한다. 전송이 끝나면 ServerHelloDone 메시지를 보내 끝났음을 알린다.

4. 클라이언트는 서버에서 받은 인증서를 검증한다. 인증서의 유효 기간이 만료되지 않았는지, 그 인증서가 해당 서버에게 발급된 인증서가 맞는지 등을 확인한다. 인증서를 신뢰할 수 있다고 판단하였다면 다음 단계로 넘어간다.

5. 클라이언트는 임의의 pre-master secret을 생성한 뒤, 서버가 보낸 인증서에 포함된 공개 키를 사용해 암호화한다. 이렇게 암호화된 pre-master secret을 ClientKeyExchange 메시지에 포함시켜 서버에 전송한다.

6. 서버는 전송받은 정보를 복호화하여 pre-master secret을 알아낸 뒤, 이 정보를 사용해 master secret을 생성한다. 그 뒤 master secret에서 세션 키를 생성해내며, 이 세션 키는 앞으로 서버와 클라이언트 간의 통신을 암호화하는데 사용할 것이다. 물론 클라이언트 역시 자신이 만들어낸 pre-master secret을 알고 있으므로, 같은 과정을 거쳐 세션 키를 스스로 만들 수 있다.

7. 이제 서버와 클라이언트는 각자 동일한 세션 키를 가지고 있으며, 이를 사용해 대칭 키 암호를 사용하는 통신을 할 수 있다. 따라서 우선 서로에게 ChangeCipherSpec 메시지를 보내 앞으로의 모든 통신 내용은 세션 키를 사용해 암호화해 보낼 것을 알려준 뒤, Finished 메시지를 보내 각자의 핸드셰이킹 과정이 끝났음을 알린다.

8. 이제 서버와 클라이언트 간에 보안 통신이 구성된다.
(구체적 설명: https://opentutorials.org/course/228/4894)

> => 서로 TLS 버전 확인 -> 인증서를 통해 신뢰성 확인 -> 암호 교환(공개키 + 대칭키) -> 암호를 이용해 통신
> => 속도는 느리지만 데이터를 안전하게 주고 받을 수 있는 공개키 방식으로 대칭키를 암호화하고, 실제 데이터를 주고 받을 때는 대칭키를 이용해서 데이터를 주고 받음
> => 데이터의 전송이 끝나면 SSL 통신이 끝났음을 서로에게 알려주고 통신에서 사용한 대칭키인 세션키를 폐기

**인증서는 누가 발급?**
통신 주체인 클라이언트와 서버의 신뢰성은 제 3자가 보증해준다. 제 3자들로는 CA(Certificate authority)라 불리우는 민간기업들이 있다. CA도 공인된 기업들만 참여할 수 있다. HTTPS 통신을 제공하려 한다면 이러한 기관들에서 인증서를 구입하면 된다.
녹색 자물쇠의 경우는 Extended Validation 인증서를 쓰는 웹사이트에 접속하면 볼 수 있는데, 이 인증서는 발급받기가 까다롭지만 공신력이 있다고 하니 안심하고 쓸 수 있겠다.

인증서에는 누가 인증서를 발급했는지 / 서비스 도메인 정보 / 서버 쪽의 공개키 내용, 공개키의 암호화 방법 등의 정보가 포함되어 있다. 이 정보 또한 CA에 의해 암호화 되는데 여기서 사용되는 암호화 기법이 공개키 방식이다. 그리고 우리가 사용하는 브라우저는 이 공개키를 이용해 인증서를 복호화하고 서버를 인증하게 된다.

2. 공인인증서
제 3자의 공신력있는 기관이 발급한, 공개키 기반의 인증서를 공인인증서라고 하지만 여기서는 '한국의' 공인인증서를 좀 더 알아보겠다.

"우리나라에는 '이 도장이 내 도장이다'고 관공서를 통해 정식으로 인증받는 '인감(印鑑)'이라는 독특한 제도가 있다. 공인인증서는 이 인감을 웹으로 옮겨둔 제도다. 사용자가 인터넷 상에서 한 거래를 '이 거래는 내가 승인한 거래다'고 인증해주는 기술이다.
공인인증서 역시 초창기 열악한 인터넷 환경에서 어떻게든 인터넷뱅킹과 전자상거래를 구현하기 위해 고안해낸 기술이다. 플러그인과 비슷하다.
초기 웹 브라우저는 암호화 능력이 부족해 해커가 중간에서 데이터를 가로채기 쉬웠다. 암호화 전송기술 자체가 없는 것은 아니었다. 넷스케이프 그룹이 95년 고안해낸 SSL(Secure Sockets Layer, https)라는 기술이 암호화 전송

기술 표준으로 각광받았다. 하지만 미국 정부의 방침 탓에 인터넷뱅킹을 구현하기엔 암호화 수준이 모자랐다. 때문에 독자적인 암호화 기술을 적용한 공인인증서를 개발해냈다. 그리고 플러그인을 사용해 공인인증서를 웹 브라우저에 적용하기 시작했다. 공인인증서와 액티브X의 밀월관계는 이렇게 시작됐다."

"국내에서 인터넷뱅킹을 하려면 사용자가 본인 인증을 받아야 한다. 미래창조과학부가 지정한 금융결제원, 한국정보인증, 코스콤, 한국전자인증, 한국무역정보통신 등 5곳의 공인인증기관이 사용자가 본인이 맞음을 인증해준다. 이 과정을 통해 발급받은 것이 바로 공인인증서다.
반면 외국의 경우 사용자는 본인 인증을 받을 필요가 없다(인터넷뱅킹에 본인 인증을 요구하는 일부 국가가 존재하긴 한다). 은행만 인증을 받으면 된다. 그렇다면 은행은 누가 인증해줄까? 국내와 다르게 국가가 아닌 공신력있는 제3자가 인증해주는 방식을 취하고 있다. 베리사인, 코모도 그룹 등이 대표적인 제3자 인증기관이다. 이러한 제3자 인증기관에서 발급한 인증서를 'EV SSL 인증서'라고 한다. SSL로 암호화된 홈페이지(URL 앞부분에 https라고 적혀 있는 홈페이지)에 접속하면, EV SSL 인증서를 통해 '누가 이 홈페이지를 인증해줬고 어느 정도로 암호화돼 있는지' 웹 브라우저를 통해 손쉽게 확인할 수 있다. 웹 표준 기술이기 때문이다."
(http://it.donga.com/17704/)

인증서를 발급 받는 주체 : 인터넷 이용자, 사용자 / 전자 거래 소비자
-> 그러나 거래가 일어나는 공간에 대한 인증은 존재 하지 않는다(피싱 사이트들이 생겨남)
-> 금융 사고가 발생해도 책임은 소비자에 있다. 공인인증서로 거래가 이루어지면 해킹을 당했다 하더라도 거래는 성립됨
-> 결론적으로 공인인증서는 문제가 되지 않는다는 것.
-> 앞으로도 공인인증서는 계속 사용될 것이고 SEED 기술 때문에 ActiveX든 또 다른 플러그 인이든 뭐든 '설치하시겠습니까?'의 지옥에서 벗어날 수 없을 것이다.

** 모든 항목을 이어보자 : ActiveX + 인터넷 익스플로러 + 웹 표준 + HTTPS + 공인인증서
2000년대 초반 한국의 상황 : 인터넷 익스프로러의 점유율 높음, 높은 속도의 인터넷 보급화
-> 인터넷을 이용하는 사람이 늘어나면서 웹 페이지도 다양한 기능들의 지원이 필요해짐
-> 대부분 인터넷 익스플로러를 사용하니 특수 기능을 지원하기 위해 ActiveX를 사용
-> 전자 거래의 경우는 웹 상의 거래를 위해선 암호화 과정 필요했다
-> 한국은 SEED라는 독자적 암호화 기술 적용한 공인인증서 개발
-> SEED는 표준이 아니어서 이 기술을 사용하기 위한 부가적 기능이 필요함
-> 이 또한 ActiveX로 제공됨. 다들 익스플로러를 쓰니까.
-> 시간은 흘러흘러 익스플로러의 점유율은 낮아지고 다양한 웹 브라우저가 등장
-> 그러나 여전히 대부분의 웹 페이지들은 익스플로러에 최적화 되어 있다(웹 표준이 지켜지지 않음)
-> 지금에서라도 웹 표준을 준수한다면 HTTPS로 안전하고 간편하게 전자 거래를 할 수 있으나 정부는 '공인인증서'를 끝까지 포기하지 못했고 더불어 ActiveX도 생명을 유지하고 있다.

결국 문제는 '공인인증서'이다. 더 정확히 말하자면 전자 거래에서 공인인증서 방식을 포기하지 않는 정책이 문제다. 왜 공인인증서를 강제하는 것일까에 대해 더 찾아보니 거기엔 금융위, 금감원, 금결원이 있었다. (링크: http://slownews.kr/11532) 기사를 요약하자면 고위 공무원들이 퇴직후 금결원의 감사로 취임해 경제적 이득을 취하고 있다. 금결원은 공인인증 사업으로 엄청난 수입을 벌고 있는 곳이기 때문에! 이 외에도 전자 거래 사고가 일어날 경우, 그 책임을 금융기관이 아닌 개인이 지고 있기 때문에 은행이나 카드사가 책임 회피를 목적으로 공인인증서를 사용하고 있다는 얘기도 있다. (http://opennet.or.kr/1789)

잘못된 정치나 정책이 개인의 삶에 미치는 영향으로 이렇게 훌륭한 예는 없다는 생각이 든다. 정치적 스트레스가 뭔지 체험해보고 싶은 사람들에게 공인인증서로 계좌이체를 시키거나 전자 등본을 떼게 해야겠다. 누군가의 이익을 위한 잘못된 정착이 고착화 되었고 이러다 고통도 고착화 되는 건 아닌지.