1주 - 2일 차 과제

소용석

➢ http와 https의 차이

1) 프로토콜명이 다르다. https의 s는 secure의 약자로 http 프로토콜에 보안 기능을 추가한 것이다.

2) http 프로토콜은 80번 포트를 사용하고 https 프로토콜은 443 프로토콜을 사용한다.

3) https의 경우, 인증을 위해 SSL 전자 서명을 필요로 한다. http의 경우에는 불요한다.

4) https의 경우에는 Transport Layer에서 암호화 과정을 거친다.

➢ 공인인증서가 생긴 배경과 그 위험성

배경: 초창기 웹 페이지들은 크고 작은 텍스트와 이미지, 그리고 하이퍼링크 정도를 표현하는 것이 다 였다. 부족한 컨텐츠를 보완하기 위해 각 웹브라우저 개발사들은 자신들의 브라우저 성능 향상을 위해 플러그인을 개발하기 시작하였고 플러그인은 인터넷의 활용도를 180도 바꾸어 상상할 수 있는 거의 모든 기능들이 구현가능하게끔 하였다. 인터넷의 부흥과 함께 플러그인도 웹 생태계에서 뗄레야 뗄 수 없는 관계가 되었다. 공인 인증서는 온라인 뱅킹 기능을 구현하는 과정에서 생겨났다. 당시 http프로토콜로 암호화 전송 기술이 마땅치 않자 (당시 https 프로토콜이 있었지만 국내에서는 사용할 수 없었다.) 플러그인 기술로 암호화 기술을 적용하여 본인의 신원을 인증할 수 있는 공인인증서가 개발되었다.

위험성: 공인인증서는 국내 은행들을 보안 안전 불감증에 빠지게 한다는 위험성을 가지고 있다. 공인 인증서 관리의 책임은 그것을 사용하는 고객에게 있었고 은행들은 요청된 은행 거래의 유효성을 단순히 공인 인증서 만으로 판별했기 때문에 은행들은 스스로 보안에 대한 인식이 취약했다. 그 결과 국내 은행은 전세계 해커들의 공격을 수시로 받았고 선량한 고객들 공인인증서 사기로 피해를 본 사례들이 많이 발생하였다.

➢ 조사하며 느낀 점

위에서 공인인증서 자체의 위험성에 대해서 작성하면서 공인인증서가 가지고 있는 잠재적인 위험성이 훨씬 더 크다는 것을 느꼈다. 국내의 많은 사용자들은 공인인증서의 위험성을 알면서도 편리함에 못이겨 지속적으로 사용을 한다. 그 결과 사용자들은 플러그인이 구현되는 환경에 스스로를 계속 가두게 되고 편향된 웹 생태계가 되게끔 한다. 하루 빨리 공인인증서 같은 구시대의 산물을 버리고 새로운 웹 표준에서 지원하는 암호화 기술을 통해 웹 접근성을 갖춘 생태계가 되어야 한다고 생각한다.