Fast Campus - 웹 프로그래밍 SCHOOL

Day 4. Homework / by. 장기수

HTTP와 HTTPS는 무엇이며 그 차이는?

HTTP와 HTTPS는 모두 HyperText를 전송하기 위한 통신규약이다. HTTPS는 Hypertext Transfer Protocol over Secure Socket Layer의 약자로 HTTPS는 Secure Socket Layer(SSL)에서 작동한다는 차이가 있음을 알 수 있다.

SSL은 공개키와 대칭키를 모두 사용하는 방법으로 대칭키를 공개키로 암호화하여 주고 받고 인증이 된 이후에 대킹키로 보안을 유지하는 방법이다. 이론상으로 완벽한 보안방법이지만 접속한 사이트가 위장하여 접근하면 문제가 발생할 수 있다. 이를 보완하기 위해 제 3의 인증기관이 등장하는데, 사이트는 인증기관으로 부터 인증서를 발급받고 사용자는 인증기관이 제공하는 공개키로 대칭키를 암호화하여 사용하는 것이다. 이렇게 인증기관에서 인증된 사이트는 브라우저에서 녹색 자물쇠 표시를 보이게 된다.

국내에 공인인증서가 생긴 배경과 그 위험성은?

인터넷 뱅킹이나 인터넷을 이용한 다양한 금융 거래들이 활발해지면서 이에 대한 보안의 필요성을 느끼고 국정원과 같은 국가기관이 보안에 대한 지침을 내리게 되었다. 문제는 국정원이 되었던 그 상위 기관이나 관련 기관이 보안 지침을 내리는데 있어서 기술적인 이슈나 향후의 미래 따위는 내다보지 않고 그저 탁상행정으로 만들어진 정책을 내렸다는 것이 문제이다. 당시 미국이 자국의 기술보호를 목적으로 해외에 제공하는 보안키를 40-bit로 제한했는데 이는 인터넷뱅킹

의 보안을 보장할 수 없었다. 이런 문제를 해결하기 위해 한국인터넷진흥원에서 SEED라는 128-bit의 키를 가지는 알고리즘을 개발하였다. 하지만 웹브라우저에서 이 기술을 지원할 방법도 이유도 없었기 때문에 라이브러리와 관련 프로그램을 배포하기 위해서 ActiveX를 사용할 수 밖에 없었다. 최근까지 ActiveX를 기반으로 공인인증서가 사용되고 있었고 오픈뱅킹을 제공하기 위해 ActiveX의 사용을 중단하였다고 하지만 대부분의 보안 프로그램들이 ActiveX를 기반으로 한 실행파일로 작동되는게 현실이다.

공인인증서는 가장 큰 문제는 보안이 무엇인지 모르는 일반 사용자들에게 개인키의 보관을 맡긴다는 것이다. 개인키는 단순한 일반 파일로 만들어져 있고 복사가 용이하여 부주의인해 유출될 수 있다. 또한 많은 사용자들이 다른 서비스와 같은 비밀번호를 공인인증서에 사용하용 있기 때문에 더더욱 심각하다.
또한 OS나 브라우저에서 제공하는 강력한 키 보관 방법을 정책적으로 지원하지 않는다는 문제도 있다.

위 내용을 조사하며 느낀 점

김인성의 IT이야기라는 웹툰을 보면서 많은 것을 배웠다. 또한 재미있고 쉽게 설명되어 있어서 시간가는줄 모르고 본 것 같다.
인상적이였던 것은 공인인증서가 OS나 브라우저에서 제공하는 키 보관 방법을 사용하지 않는 것이였는데 한국의 정치와 경제에 얽매인 썩어빠진 행정을 보게 되어 크게 낙담할 수 밖에 없었다.

더욱 공부해야 함을 느낀다.

참조.

과제 1.
http://naramoksu.tistory.com/2143330
http://minix.tistory.com/397

과제 2.

https://namu.wiki/w/%EA%B3%B5%EC%9D%B8%EC%9D%B8%EC%A6%9D%EC%84%9C

http://minix.tistory.com/403