Day4. Computational Thinking_4

전미정

Q1. HTTP와 HTTPS는 무엇이며 그 차이는?

A1. HTTP 는 Hypertext Transfer Protocol 의 약자로, Hyper Text 인 HTML 을 전송하기 위한 통신규약을 의미하며, HTTPS 는 Hypertext Transfer Protocol over Secure Socket Layer 의 약자로, HTTP 의 보안이 강화된 버전이다. 기존에 사용된 HTTP 는 데이터가 암호화되지 않은 방법으로 전송되기 때문에 중간에서 제 3 자가 메시지를 감청하거나 변조하는 일이 발생할수 있다. 이러한 일을 방지하기 위해 데이터를 암호화 하는 일이며, 보완이 중요한 은행이나 쇼핑몰, 정부사이트 등에서 HTTPS 를 사용하고 있다.
HTTP 는 속도가 빠르고 재접속시 로딩 화면을 그대로 불러들어 많은 국내 사이트에서 사용되고있다. HTTPS 는 암호화된 정보를 교환해야하기 때문에 서버에 과부하가 걸리는 경우가 많고, 접속이 끊기게 되면 처음부터 다시 시작해야하는 불편함이 있어 널리 사용되지 않고있다.

Q2. 국내에 공인인증서가 생긴 배경과 그 위험성은?

A2. 인터넷이 널리 보급되고 인터넷 뱅킹이 시작 되던 1990 년대 후반, 한국에서는 미국의 웹 브라우저를 수입해서 사용했는데 이 당시 미국은 자국 기술보호를 이유로 자신들은 128 비트 수준의 보안을 사용하지만 수출용 웹브라우저는 40 비트로 수준을 제한시켰다. 하지만 40 비트 암호화 기술은 실시간으로 해킹되는 취약한

시스템으로, 뱅킹 시스템에 적용하기에는 한계가 있었다. 그래서 한국인터넷진흥원에서 자체적의로 128 비트짜리 대칭키 블록 암호화 알고리즘 SEED 를 개발하였다. SEED 를 웹브라우저에서 사용하기 위해 ActiveX 를 이용하게 되었으며, 이것이 대한민국 ActiveX 와 공인인증서의 시작으로 대한민국 인터넷 환경을 취약하게 만드는 주범이 되었다. 공인인증서를 사용하는 것으로 인한 문제점으로는 파일의 복사 가능성, 사용자 자체 관리, 사용 비용 그리고 의무 사용에 있다. 이러한 공인인증서는 뱅킹 시스템 구축에 반드시 필요한 것이 아니므로 사라져야 하는것이 마땅하나, 관련 기업과 기득권의 횡패로 쉽게 사라지지 않고있다.

Q3. 위 내용을 조사하며 느낀점

A3. 우리나라 공인인증서의 문제점을 다시 한번 파악하게 되었으며, 인터넷에서 왜 보안이 중요할 수 밖에 없는지를 알게 되었다. 그리고 또 하나 중요한 점은 빠르게 변하는 IT 시장을 읽을 수 있어야 하며, 더 나은 기술을 빠르게 채택하는 개발자가 되어야 한다는걸 느낄 수 있었다.
공인인증서 만료기간이 지났는데...앞으로 직구를 많이 활용해야겠다.