<Day3 Homwork>

작성자 : 김영환

1. HTTP와 HTTPS는 무엇이며 그 차이는?

>

HTTP와 HTTPS는 클라이언트와 서버 간에 쓰이는 통신 프로토콜이다. 둘 다 HTML 문서를 주고받는다는 특성이 있으나, HTTPS는 SSL 을 지원하기 때문에 전송되는 정보가 암호화되어 전송된다.

다만 단점으로는 서버에 부하가 걸린다는 점과 캐시를 쓸 수 없기 때문에 인터넷 접속 환경이 불안정하면 유저의 짜증을 유발할 수 있다.

2. 국내에 공인인증서가 생긴 배경과 그 위험성은?

>

마이크로소프트는 과거 IE 에 40비트 수준의 낮은 보안접속만 지원했다. 이는 국내 유저들의 인터넷 보안에 심각한 문제를 줄 가능성이 있었다. 때문에 정부에서는 국내 암호화 표준으로 자체개발한 SEED 알고리즘을 채택한다. 이 과정에서 액티브X 를 구현 기술로 차용했으며, 이렇게 만들어진 '공인인증서'는 법적으로 이용이 의무화 되었다.

액티브X 는 브라우저를 기반으로 하나 윈도우 내부 파일 삭제, 조작, 레지스트리 변경 등이 가능했기 때문에, 심각한 보안 위험성이 있었다. 그러나 정부에서는 법안으로 정한 공인인증서 의무사용을 검토하지 않았고, 잠재적 위험요소로서 남게 되었다.

3. 위 내용을 조사하며 느낀 점

>

HTTP나 공인인증서는 유저의 보안과 관련한 부분이다. 보내는 HTML 문서를 암호화 할 것이냐, 유저의 인증을 액티브X 로 할 것이냐하는 이슈는 단기적으로는 큰 문제가 없어보인다. 그러나 잠재적 보안 허점을 노출하여 해커의 표적이 되며, 더 큰 문제는 이미 개발환경이 저 두 가지를 쓸 수 밖에 없도록 고정되어 있다는 점이다. 일부 서비스는 HTTPS를 지원하지만, 아직도 대부분의 서비스는 HTTP 기반이다.

안전과 비용은 트레이드오프 관계다. 그러나 당장의 비용보다는 좀 더 미래의 문제점을 고려해야 하며, 이는 훌륭한 프로그래머, 아키텍트, 혹은 프로젝트 기안자가 생각해야 할 문제라고 할 수 있다.