FAST CAMPUS ios dev school 과제 4

박상욱

HTTP 와 HTTPS 는 무엇이며 그 차이는?

HTTP 는 Hypertext Transfer Protoco 의 약자로 Hypertext 로 되어져 있는 HTML 을 전송하기 위해 만들어진 통신규약이다. HTTPS 는 위 내용을 기반으로 SSL(Over Secure Socket Layer), 즉 보안이 강화된 HTTP 포맷이다.

HTTP	HTTPS
필요한 정보를 서버에서 불러와 사용자에게 제공함 **서버 네트워크를 통해 보안정보를 가로챌 수 있는 경우가 발생함** **접속이 끊기더라도 즉시 데이터 로드가 가능함**	**보안이 강화됨** 전자상거래에 주로 사용됨 데이터 보호를 어느정도 보장함 암호화 알고리즘에 따라 보호수준이 나뉨 **서버가 과부화되면 처음부터 다시 해야함**

국내에 공인인증서가 생긴 배경과 그 위험성은?

1991 년 전자서명법을 제정하여, 행정안전부가 지정한 공인인증 기관에서 발급 받아 본인인증을 함으로서 온라인 금전거래가 가능하도록 허용하는 제도이다. 90 년대 당시 미국이 보안 프로그램을 수출하지 않자, Active X 와 마찬가지로 독자적으로 구축을 하게 되었다. 기존보다 더 고도화된 암호화 모듈을 사용하고 있는데, 이는 강제적으로 국민들이 사용하지 않는 이상 상용화되기 어렵다고 판단되어 공인인증이라는 명목으로 만들어졌다. 하지만, 미국이 이 이후 곧바로 수출 규제를 완화 시켰고, 여기서 우리나라가 고도화된 암호를 ActiveX 로 자체 플러그인을 설치하는 것을 제외하고 대응할 방법이 없자, 플러그인을 깔도록 유도하였다. 여기서 부터 단점이 나타나는데, 컴퓨터를 사용하는 유저들이 부가 프로그램을 설치해야해서 보안 경고를 무시하는 경우가 잦아진다. 그 외에도 인증서 암호를 동일하게 하기 때문에 해킹당했을 경우 타 계정 암호는 쉽게 노출이 된다. 그 외에도 공인인증서는 누구든지 온라인으로 발급이 가능하기 때문에 개인의 정보만 있으면 바로 유출될 위험이 있다.

위 내용을 조사하며 느낀점

국내 IT 환경을 형성해 나간 것에 대해선 정말 멋진 일이라고 보지만, 개인적으로 지금까지 공인인증서를 쓴다는 것은 말이 안되며, 조금 더 이러한 프로그램에 대한 개선 인식이 정부 내에서 많이 개선되야 하지 않을까 싶다.