HTTP와 HTTPS는 무엇이며 그 차이는?

WWW상에서 정보를 주고 받는 프로토콜 입니다.

그렇다면 WWW이 무엇인가? World Wide Web약어로써 인터넷으로 연결된 컴퓨터를 매개체로 사람들간에
정보를 나누고 공유할 수 있는 공간입니다. 간혹 Web이라는 단어의 뜻과 혼동될 수 있으나 Web이란 하나의 인터넷서비스라고 할수 있습니다.
다시돌아와서 HTTP란 프로토콜인데 이 프로토콜의 역할은 클라이언트와 서버간에 요청과응답을 수행하는 프로토콜입니다.

만약 사용자가 서버측으로 보고싶은 사진을 누릅니다(HTTP 프로토콜을 통해 요청)
서버는 요청을 받아 사용자가 요구한 사진을 다시 사용자에게 보냅니다(HTTP프로토콜을 통해 응답)

장점으로는 접속이 끊기더라도 재연결 되었을 때 다시 시작할 필요업이 바로 마지막페이지를 보여줍니다.

단점으로는
클라인언트가 요청한 페이지를 암호가 안된 상태로 정보를 교환 할 수있어서 그 중간에 들어와 정보를 빼갈 수 있어서 보안에 약한점을 가지고 있습니다.

HTTPS란 무엇이고 어떠한 점이 다른가?

HTTPS는 HTTP에서 보안이 강화된 프로토콜이라고 할 수 있습니다. 그래서 주로 인증이나 전자거래, 결재시스템의 웹페이지에서 볼 수 있습니다. 만약 HTTPS를 사용하여 통신을 하는 웹페이지라면 http://~ 가 아니라 https://~로 주소가 시작되는 것을 보며 어떤 프로토콜로 웹페이지가 요청받고 응답받는지 알 수 있습니다.

HTTP보다 보안이 강화되었지만 이 또한 단점이 존재합니다. 암호화정보를 주고받기때문에 보안성이높지만 그만큼 서버가 부담이커서 많은 접속자가 요청을 한다면 서버에 과부화가 걸릴 수 있으며 접속이끊긴다면 처음부터 다시 시작해야 합니다.

- 국내에 공인인증서가 생긴 배경과 그 위험성은?

공인인증서는 인터넷에 상에서 사람의 주민등록증같은 역할을 합니다. 중요한 것은 공인인증서는 그냥 데이터 파일에 불과한다는 것입니다. 그러나 이것을 보고 공인인증서를 인증 하려면 그것을 수행할 프로그램이 필요했습니다. 이때 우리나라는 어제 조사한 바와 같이 윈도우세상이기 때문에 Active-x기반으로 인증프로그램을 개발했습니다. 그러나 Active-X를 설치할 때악성코드가 같이 설치하게 할 수도 있었기 때문에 보안에서 문제점이 있었습니다. 하지만 그 당시에는 그것을 사람들은 느끼지 못했었습니다. 또한 Active-X는 IE에서 밖에 사용이 안되니 다른 타 브라우저와도 호환이 어려웠습니다.

이런 Active-X로 인한 보안에 대한 구멍과 호환에대한 제한도 있었지만 또다른 위험성은 일반저장매체에 공인인증서를 저장시킬 수 있는 점입니다. 도입초기에 보편적이고 빠르게 보급하기 위해서 일반 저장매체에 복사붙여넣기가 가능하도록 허용하여서 해킹이나 정보를 유출시킬 수있는 환경을 키웠습니다. 또한 재발급이 쉽다는 것입니다. 인증서자체는 암호를 푸는게 어렵지만 재 발급은 쉬우니 다시 재발급받아서 악용될 수 있는데 이것또한 인증서의 위험서을 높이는 요소 중 하나 입니다.

- 위 내용을 조사하며 느낀 점

2일차에 기술적부채라는 것을 조사했습니다. 공인인증서또한 Active-X라는 것에 발목잡혀서 시대흐름을 따라가지 못하고 구멍을 생기게 했고 제대로 활용도 못하게 된 것 같습니다. HTML5기반으로 공인인증서기술을 개발한다면 Active-X보다 안전하고 다른 브라우저와도 호환가능한데 아직 이런 움직임이 미미해서 조사하는 와중 안타까웠습니다. 어서 국제표준에 맞게 다시 기술이 개발되었으면 좋겠다고 느꼈습니다.