1. HTTP/HTTPS-HTTP와 HTTPS는 무엇이며 그 차이는?

:: HTTP (위키백과사전 HTTP 참조)

인터넷에서 하이퍼텍스트(hypertext) 문서를 교환하기 위하여 사용되는 통신규약이다. 하이퍼텍스트는 문서 중간중간에 특정 키워드를 두고 문자나 그림을 상호 유기적으로 결합하여 연결시킴으로써, 서로 다른 문서라 할지라도 하나의 문서인 것처럼 보이면서 참조하기 쉽도록 하는 방식을 의미한다.

http는 1989년 팀 버너스 리(Tim Berners Lee)에 의하여 처음 설계되어 인터넷을 통한 월드 와이드 웹(World-Wide Web) 기반에서 전 세계적인 정보공유를 이루는데 큰 역할을 하였다. http의 첫번째 버전은 인터넷을 통하여 가공되지 않은 데이터를 전송하기 위한 단순한 프로토콜이었으나, 데이터에 대한 전송과 요구·응답에 대한 수정 등 가공된 정보를 포함하는 프로토콜로 개선되었다.

인터넷 주소를 지정할 때 'http://www....'와 같이 하는 것은 www로 시작되는 인터넷 주소에서 하이퍼텍스트 문서의 교환을 http 통신규약으로 처리하라는 뜻이다.

:: HTTPS (위키백과사전 HTTPS 참조)

https란 인터넷 상에서 정보를 암호화하는 SSL(Secure Socket Layer) 프로토콜을 이용하여 데이터를 전송하고 있다는 것을 의미한다. SSL 프로토콜은 테리사(Terrsa)가 개발해 Netscape사가 NetSite의 암호화 중심 프로토콜로 정착시킨 기술로 정보 암호화시 공개키(Pubilc Key)와 개인키(Private Key)라는 두 가지 키를 이용하는 방법이다.

공개키(Public Key)는 인터넷 상에 공개되어 있는 키로 서버에서 자동으로 이용자의 브라우져로 보내며, 이용자가 입력한 정보는 이 공개키(Public Key)를 이용하여 암호화되어 다시 서버까지 전달된다.

이 공개키(Public Key)로 암호화된 정보는 서버만이 유일하게 소유하고 있는 개인키(Private Key)로만 해독이 가능하다.

제3자가 의도적으로 암호화된 이용자 정보를 가로챈다 하더라도, 서버의 개인키(Private Key)가 없는 한은 해석이 불가능하다는 것을 의미한다.

:: HTTP와 HTTPS의 차이

http와 https의 약자를 살펴보면 SSL(Secure Socket Layer)를 쓰는가 아닌가의 차이임을 알 수 있다.

•http : HyperText Transfer Protocol

•https : Hypertext Transfer Protocol over Secure Socket Layer

이에 따라 동작 순서에도 차이가 있는데 그 순서는 다음과 같다.

•HTTP : TCP -> HTTP

•HTTPS : TCP -> SSL -> HTTP

2. 공인인증서 - 국내에 공인인증서가 생긴 배경과 그 이유는?

국내 대부분의 금융, 게임, 포털 사이트가 액티브X를 통해 결제·전자서명·파일 교환 등의 서비스를 제공하여 사용자들이 익스플로러 대신 다른 브라우저를 쓰는 게 거의 불가능한 상태였다. 또한 초창기 웹 브라우저는 그 기능이 미약했다. 텍스트와 이미지만 읽을 수 있었고, 동영상 재생같 은 것은 꿈도 꾸지 못했다. 암호화는 배부른 소리였다. 이처럼 초기 웹 브라우저는 암호화 능력이 부족해 해커가 중간에서 데이터를 가로채기 쉬웠다. 암호화 전송기술 자체가 없는 것은 아니었다. 넷스케이프 그룹이 95년 고안해낸 SSL(Secure Sockets Layer, https)라는 기술이 암호화 전송기술 표준으로 각광받았다. 하지만 미국 정부의 방침 탓에 인터넷뱅킹을 구현하기엔 암호화 수준이 모자랐다. 때문에 독자적인 암호화 기술을 적용한 공인인증서를 개발해냈다. 그리고 플러그인을 사용해 공인인증서를 웹 브라우저에 적용하기 시작했다.

3. 위의 내용을 조사하면서 느낀 점

http와 https에 대해 그 의미만 들어보았을 땐, http사이트, https사이트 이렇게 따로 있구나 생각했었다. 하지만 조사를 하며 알게 된 점으로는 다음이나 네이버 등은 그 사이트는 http로 되어있고, 내부 소스 action만 https로 보내는 방식(로그인창 http, 로그인처리 https)으로 혼용 구성하여 사용한다는 것이 흥미로웠다. 매일 보는 네이버만 해도 메인 주소는
http://www.naver.com/
http인데, 검색하며 페이지를 이동하면
https://search.naver.com/search.naver?sm=tab_hty.top&where=nexearch&ie=utf8&query=%EC%BB%B4%ED%93%A8%ED%84%B0%EA%B0%9C%EB%A1%A0
위와 같은 방식으로 https로 바뀌고 있었다. 이렇게 혼용으로 http와 https를 구성한 웹페이지들의 주소를 유심히 보며 어떤 부분에서 보안이 필요한 것인지 유추 해 볼 수 있을 것 같다.
예를 들어 같은 검색을 해도 네이버 사전 검색에서는
http://frdic.naver.com/koreaEntry.nhn?entryNO=819340
이와 같이 http로 페이지를 제공하고 있었다. 앞으로도 단순히 웹페이지를 정보를 얻기 위한 수단만으로 생각하지 않고 웹 프로그래머를 지망하는 이의 입장으로 하나하나 유심히 살펴봐야겠다는 생각이 들었다.

요즘은 이전과제에서 ActiveX를 조사하며 빼놓지 않고 같이 맞물려 나왔던 이야기가 공인인증서에 대한이야기와 더 나아가 이를 대체 할 인증방법에 대한 이야기였다. 이를 조사하며 생체인식에 대한 관심과 기대가 커졌으나, 또한 이전 과제에서 웹 접근성을 조사하며 다양한 특성을 가진 사람들을 배려해야하는데 어떠한 방법으로 이를 제공할지가 가장 궁금하였다. 앞으로도 공인인증서를 대체 할 인증방법에 대해 관심을 가지고 지켜보고자 한다.