http란?

인터넷에서 하이퍼텍스트문서를 교환하기 위하여 사용되는 통신규약입니다. 하이퍼텍스트는 문서 중간중간에 특정 키워드를 두고 문자나 그림을 상호 유기적으로 결합하여 연결시킴으로써, 서로 다른 문서라 할지라도 하나의 문서인 것처럼 보이면서 참조하기 쉽도록 하는 방식을 의미합니다. 일종의 대화 규칙이며, 교환방식은 바이너리 데이터가 아닌 단순 텍스트를 통해 이루어집니다.

1989년 팀 버너스 리에 의하여 처음 설계되어 인터넷을 통한 월드 와이드 웹기반에서 전 세계적인 정보공유를 이루는데 큰 역할을 합니다. http의 첫번째 버전은 인터넷을 통하여 가공되지 않은 데이터를 전송하기 위한 단순한 프로토콜이었으나, 데이터에 대한 전송과 요구·응답에 대한 수정 등 가공된 정보를 포함하는 프로토콜로 개선되었습니다.

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

https란?

https 란 인터넷 상에서 정보를 암호화하는 SSL(Secure Socket Layer) 프로토콜을 이용하여 데이터를 전송하고 있다는 것을 의미합니다. SSL 프로토콜은 넷스케이프가 NetSite의 암호화 중심 프로토콜로 정착시킨 기술로 정보 암호화시 공개키(Pubilc Key)와 개인키(Private Key)라는 두가지 키를 이용하는 방법입니다.

공개키(Public Key)는 인터넷 상에 공개되어 있는 키로 서버에서 자동으로 이용자의 브라우져로 보내며, 이용자가 입력한 정보는 이 공개키를 이용하여 암호화 되어서 다시 서버까지 전달됩니다.

이 공개키로 암호화된 정보는 서버만이 유일하게 소유하고 있는 개인키(Private Key)로만 해독이 가능합니다. 제3자가 의도적으로 암호화된 이용자 정보를 가로챈다 하더라도, 서버의 개인키가 없는 한 해석이 불가능합니다.

덧붙여 SSL은 점차 폭넓게 사용되다가 표준화 기구인 IETF의 관리로 변경되면서 TLS라는 이름으로 바뀌었습니다. TLS 1.0은 SSL 3.0을 계승하지만 TLS라는 이름보다 SSL이라는 이름이 훨씬 많이 사용되고 있습니다.

차이점

http의 보안 취약점을 보완한 것이 https입니다. https에서 마지막의 S는 Over Secure Socket Layer의 약자로 Secure라는 말을 통해서 알 수 있듯이 보안이 강화된 http라는 것을 짐작할 수 있습니다. 물론 이 암호를 풀수는 있지만 어마어마어마어마한 시간이 걸립니다. 그래서 보다 안전하다 할 수 있습니다.

https가 안전하면 모두 https를 사용하면 되는데, 왜 http를 사용하는지에 대해 의문이 생길 수 있습니다. https 암호화를 하려면 웹 서버에 부하가 생기고 위에서 암호키가 그 서버의 인증서가 되는데, 이것은 Verisign 같은 업체에서 비싼 돈을 주고 사야하므로, 특히 우리나라 웹 사이트들은 잘 사용하지 않습니다.하지만 외국 금융 사이트에서는 https는 필수입니다.

http는 비연결형으로 웹 페이지를 보는 중 인터넷 연결이 끊겼다가 다시 연결되어도 페이지를 계속 볼 수 있지만 https의 경우에는 소켓(데이터를 주고 받는 경로) 자체에서 인증을 하기 때문에 인터넷 연결이 끊기면 소켓도 끊어져서 다시 https 인증을 해야 하기 때문에 시간이 또 걸릴 수 있습니다.

국내에 공인인증서가 생긴 배경과 이유

공인인증서란 쉽게 말해 전자 인감도장입니다. 공인인증서는 이 인감도장을 웹으로 옮겨둔 제도입니다. 사용자가 인터넷 상에서 행한 거래를 본인의 승인으로 이루어진 거래임을 증명해 주는 기술입니다. 공인인증서 역시 플러그인과 마찬가지로 열악했던 인터넷 환경에서 어떻게든 인터넷뱅킹과 전자상거래를 구현하기 위해 고안해낸 기술입니다.

초창기 웹 브라우저는 암호화 능력이 부족해 해커가 중간에서 데이터를 가로채기 쉬웠습니다. 데이터를 암호화할 필요가 있었습니다. 물론 암호화 전송기술 자체가 없는 것은 아니었습니다. https라는 기술이 암호화 전송기술 표준으로 각광받긴 했습니다. 하지만 미국 정부의 암호화 보호 방침 탓에 우리나라는 인터넷뱅킹을 구현하기엔 암호화 수준이 부족했습니다. 때문에 독자적인 암호화 기술을 적용한 공인인증서를 개발이 필요했습니다. 그리고 플러그인(액티브X)을 사용해 공인인증서를 웹 브라우저에 적용하기 시작했습다. 대한민국 웹의 비극은 이렇게 시작됐습니다.

전자거래에서 공인인증을 법제화했고 이 공인인증은 IE의 액티브X에서만 동작했습니다.

MS의 천국인 우리나라에서 모든 공인인증절차는 액티브X 없이는 불가능 했습니다. 개발이 편리하고 다향한 성능을 구현할 수있다는 장점 때문에 강력히 입지를 굳힌 액티브X와 공인인증의 만남은 보안의 취약점이 드러난 이후에도 시들지 않았습니다.

사실 공인인증서도 SSL과 비슷한 원리입니다. 다만 사용자 인증이냐 서버인증이냐 차이입니다. 우리나라의 공인인증서는 보안에 취약하기 쉬운 개인 사용자에게 그 책임을 모두 떠넘겼습니다.

악성코드를 통해 발각되기 쉬운 개인키(일정한 디텍토리에 저장돼있어 쉽게 접근할 수 있습니다), 수많은 이용자를 확보하고 있지만 보안은 허술한 사이트들을 털어 얻어낸 사용자들의 비밀번호, 그리고 허술한 보안의식을 노려 공인인증서와 같은 비밀번호를 쓰는 사용자를 찾아내는건 너무나 쉬운일이었습니다. 또 멀리 갈 필요 없이 주변사람이 악용할 위험성도 있습니다. 그냥 파일을 복사하면 되니까요.

이후 그 피해를 모든 국민이 떠안았습니다. 중국에서 대한민국 국민의 개인정보가 헐값에 거래된다는 것은 지상파 뉴스에도 나올말큼 이미 공공연한 비밀입니다.

느낀점

개인 사용자에게 보안책임을 묻는 행태가 너무 뻔뻔해서 다시 분개 할 수 밖에 없습니다.

인터넷뱅킹에서 공인인증서를 의무적으로 사용하도록 했던 규정이 폐지됐다는 소식을 듣고 '해결된건가?!'싶었지만 결국 '정부는 손 땔테니 너희들끼라 알아서 해라'라는 것이었습니다. 칼자루가 법원의 손에 쥐어졌지만 어떻게 될지는 여전히 의문으로 남습니다. 답답하기는 매한가지 였습니다.

그리고 문득 이런 생각이 들었습니다. 결국 일선의 실무자들이 소명을 가지고 일해야 하지 않을까. 위에서 아무리 위에서 푸쉬를 해도 최소한의 원칙을 지켜야 한다는 본보기로 이 상황을 새겨야겠다는 생각이 들었습니ㅉ다.