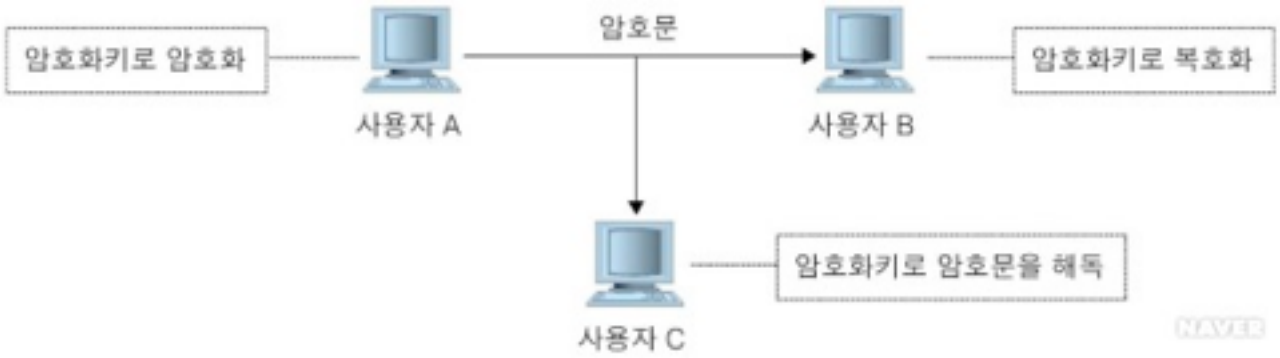
1. HTTP vs HTTPS

HTTP

HTML과 같은 문서를 웹 브라우저가 웹 서버에 요청하는 일종의 규칙입니다. HTTP는 웹브라우저와 웹 서버간의 규칙이므로 서로간의 규칙에 맞게 데이터를 교환합니다. 단순한 데이터 교환이기 때문에 만약 네트워크 상에 그 신호를 가로챈다면, 교환이 일어나는 데이터를 볼 수 있게 됩니다.

HTTPS

HTTPS는 HTTP의 보안적인 취약점을 보완한 프로토콜입니다. HTTPS의 S(secure socket)의 의미처럼 안전하게 암호화되어 데이터를 전송합니다. HTTPS에서는 SSL 프로토콜을 사용는데, SSL 프로토콜은 암호화 중심 프로토콜로 암호화시 공개키(Pubilc Key)와 개인키(Private Key)라는 두가지 키를 이용하는 방법입니다.



공개키 암호화 방식에 대해서 간단하게 설명하면, 위 사진에서 사용자 A가 클라이언트, 사용자 B가 웹서버가 됩니다.
공개키(Public Key)는 인터넷 상에 공개되어 있는 키로 서버에서 자동으로 사용자 A(클라이언트)로 보내며, 이용자가 입력한 정보는 이 공개키(Public Key)를 이용하여 암호화되어 사용자 B(웹서버)까지 전달됩니다. 이 공개키(Public Key)로 암호화된 정보는 사용자 B(웹서버)만이 유일하게 소유하고 있는 개인키(Private Key)로만 해독이 가능합니다. 제3자가 의도적으로 암호화된 이용자 정보를 가로챈다 하더라도, 서버의 개인키(Private Key)가 없는 한은 해석이 불가능하다는 것입니다.
만약 중간에 1024비트 암호화를 사용한 암호를 풀려고 2의 1024승의 가지수가 생기며, 절대적으로 엄청난 시간이 걸리게 됩니다.

2. 공인인증서 - 국내에 공인인증서가 생긴 배경과 그 이유는?

해외의 경우 개인에 대한 증명을 확인하는 방법이 이메일인증이 대부분입니다. 허나 우리나라의 경우, 짝퉁 이메일이 많아 이메일을 인증 수단으로 사용하기 어려웠고 이에따라 개인에 대한 증명을 할 수 있는 공인인증서를 만들게 되었습니다.

허나 많은 고민 끝에 탄생한 공인 인증서는 빈틈이 많았습니다.

국내 공인인증서의 경우, 공인 인증서를 개인이 하드나 USB 혹은 핸드폰 등에 저장해야 하므로 별도의 프로그램이 필요하다는 점입니다. 또한 하드디스크나 USB의 경우 PC에 연결되는 특성 상 데이터를 읽을 때 중간에 관련된 내용을 가로채 메모리 해킹에 취약하게 됩니다.
이외에도 보안적으로 취약한 Active X로 공인인증서를 사용해야 하는 것이 있습니다. 최근에는 멀티 플랫폼으로 가려고 하는 추세이나 여전히 많은 은행들이 Active X 기반으로 공인인증서 시스템을 구축하고 있습니다.

3. **위 내용을 조사하면서 느낀 점**

위 내용을 조사하기 전에는 무조건적으로 Active X와 공인인증서에 대해서 부정적인 의식을 가지고 있었습니다. 허나 공인인증서가 도입 된 역사를 보면서, 그 당시의 이슈를 해결하기 위한 최선의 방법일 수도 있다는 생각이 들었습니다. 물론 지금은 전세계 웹 표준에 못따라가고 있는 현실이지만, 조금 더 고민하여 전세계 웹 표준을 지키면서 보안도 강화할 수 있는 방안을 마련했으면 하는 바람입니다.