HTTP와 HTTPS 의차이

HTTP(Hyper Text Transfer Protocol)는 주로 HTML 문서를 주고 받는데 사용한다. TCP와 UDP를 사용하여 80번 포트를 사용한다. 1996년 버전 1.0 그리고 1999년 1.1 이 각각 발표되었으며, 현재 가장 널리 쓰이는 버전이 1.1이다. HTTP는 클라이언트와 서버사이에서 이루어지는 요청 응답 프로토콜이다. 예를들면 클라이언트인 웹 브라우져가 HTTP를 통하여 서버로부터 웹페이지나 그림 정보를 요청하면, 서버는 이 요청에 응답하여 필요한 정보를 해당 사용자에게 전달하게 된다. 이 정보가 모니터와 같은 출력 장치를 통해 사용자에게 나타나는 것이다.

HTTP를 통해 전달되는 자료는 http:로 시작하는 URL(인터넷주소)로 조회할 수 있다.

HTTPS는 HTTP+SSL로 암호화된 http 프로토콜이다. http는 평문으로 통신되게 때문에 통신구간 도청이나 위,변조 공격에 취약하다. 반면 http는 암호통신이기 때문에 안전하다. 최근 EV-SSL 개념이 웹 브라우저에 탑재되어 EV-SSL인증서를 사용하는 웹사이트에 접속 시 웹 브라우져 주소 창이 녹색으로 변하기 때문에 사용자 입장에서 쉡게 https를 식별할 수 있는 장점을 갖는다. http는 이런 HTML 같은 문서를 웹 브라우져가 웹 서버에 요청하는 프로토콜이다.프로토콜이라는 것은 일종의 대화 규칙이다. 우리가 폰 뱅킹할 때 지정된 코드를 누르면 정해진 응답이 온다. 이게 없다면 웹 서버는 웹 브라우저가 무슨 페이지를 달라고 하는 건지도 모를 것이고 웹 브라우저도 웹 서버가 무슨 페이지를 보내는 건지 알 수가 없다. Http도 그냥 텍스트 교환일 뿐이다. 복잡한 바이너리 데이터가 아니라 그냥 텍스트 메시지를 주고 받는 것이다. 물론 그 텍스트 메시지 안에 HTML 페이지도 들어 있다. 텍스트이기 때문에 만약 내가 있는 네트워크 안에서 누가 그 신호를 가로채어 본다면 내용이 그대로 보이게 된다. 만약 내가 메일을 읽고 있는데 누가 그 신호를 가로챈다면 메일 내용을 읽을 수 있을 것이다. https는 http하고 거의 같지만 모든 통신 내용을 암호화하는 것이 다르다. 사실 s가 secure socket, 즉 안전한 통신망을 뜻한다. 우리는 파일에 암호를 많이 걸어 봤을 것이다. 어떤 키를 설정해서 걸면 나중에 풀 때에도 그걸 입력해 푸는 것이다. 키라는 것은 암호화를 푸는 암호 즉 패스워드 같은 것이다. 웹 서버가 키 하나를 정해서 페이지를 암호화해서 사용자의 웹 브라우저로 보내고 웹 브라우저는 그 키를 이용해서 페이지를 복원할 수 있으면 좋겠지만 그렇게 간단하지 않다. 웹 서버는 하나이지만 사용자는 불특정 다수이다. 그런데 키를 사용자들에게 줘 버리면 아무나 암호화를 풀 수 있게 된다. 영희에게 갈 페이지를 철수도 풀어서 볼 수 있게 되는데, 이러면 암호화의 효과가 없다.

 즉, 페이지 암호화 키가 그 페이지를 보는 특정 사용자에게만 알려져야 한다. 그러면 어떻게 할 수 있을까? 이것이 바로 https 프로토콜이 하는 일이다. 위에서 말한 암호화 방식을 사용하되, 그 키를 다시 공개키로 암호화하고 인증하는 것이다. 공개키는 쉽게 말해서 데이터를 암호화하는데 키가 두개 필요하다는 것이다. 암호화를 푸는 데에는 그 두 개 중 하나의 키만 있으면 된다. 한 사이트에서는 A, B라는 키를 가지고 있다. 그리고 이 B라는 키만 사용자들에게 알려준다. 그리고 한 사이트에 웹 브라우저가 연결을 시도할 때, 파일 암호화 키를 이 A, B 키로 암호화해서 보내 준다. 그러면 사용자들은 B라는 키로 데이터를 풀어볼 수 있다. A는 해당 사이트 관리자 말고는 아무도 모르기 때문에, B만 알아서는 해당 사이트와 똑같이 암호화를 할 수 없다. 즉 사용자는 B로 풀어봐서 풀어지면 이 데이터는 A키를 아는 해당 사이트 관리자가 암호화한 것이라는 걸 알 수 있는 것이다. http 프로토콜의 경우 중간에서 네트워크 데이터를 가로채서 마치 자기가 해당 사이트인 것처럼 해서 가짜 페이지를 보낼 수도 있을 것이다. 하지만 https의 경우에는 A키를 모르기 때문에 중간에서 누가 그렇게 할 수가 없다. 이렇게 해서 반대편이 해당 사이트라는 것을 우리는 믿을 수 있다. 이렇게 믿을 수 있으면 IE같은 브라우저에서는 주소 창의 색을 다르게 해서 안전하다고 알려준다. 이렇게 해서 웹 서버와 사용자가 교환한 키로 전체이후로는 HTML을 암호화해서 교환하는 것이다. 이렇게 되면 중간에서 웹 페이지를 누가 가로채도 내용을 전혀 읽을 수 없다. 사실 시간이 주어진다면 암호화를 풀 수도 있다. 예를 들어 1024비트 암호화를 사용한다면 암호 키가 1024비트, 즉 2의 1024승이라는 것이다. 암호를 계산해서 푸는 방법은 없다. 키를 모르고 암호화를 푼다는 것은 모든 키를 하나씩 다 대입해서 풀릴 때까지 해 보는 것이다. 그러면 위의 경우 평균적으로 2의 512승 번을 해봐야 한다. 2의 512승과 2x512는 차원이 다르다. 2의 20승만 해도 백 만이 넘는다. 아무리 빠른 컴퓨터로 대입해도 아마 몇 천 년은 해야 할 것이다. 그래서 안전하다고 할 수 있다. 그러면 https가 안전하면 모두 https를 사용하면 되는데, 왜 http를 사용하는지에 대해 의문을 가질 것이다. https 암호화를 하려면 웹 서버에 부하가 생기고 위에서 말한 B가 그 서버의 인증서가 되는데, 이것은 Verisign 같은 업체에서 비싼 돈을 주고 사야하므로, 특히 우리나라 웹 사이트들은 잘 사용하지 않는다.

 하지만 외국 금융 사이트에서는 https는 필수이다. 또 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 있다.

공인인증서는 전자 서명의 검증에 필요한 공개 키에 소유자 정보를 추가하여 만든 일종의 전자 신분증이다. 공개키 증명서, 디지털 증명서, 전자 증명서 등으로 불린다. 공인인증서는 개인 키와 한쌍으로 존재한다.

공인인증서는 OpenSSL의 ssl-ca나 수세 리눅스의 gensslcert와 같은 도구를 포함한 유닉스 기반 서버용으로 작성되었다. 비대면 온라인 방식의 전자상거래에서 상대방과의 계약서 작성, 신원 확인 등에 전자서명이 필요하며 동시에 공인인증서로 해당 전자서명을 생성한 자의 신원을 확인하게 된다.

공개키 기반 구조(PKI)는 전자 서명을 생성하고 검증하는데 사용되는 개인키와 공개키를 안전하게 나누어주는 역할을 담당하는 신뢰된 제 3자의 존재를 전제로 하고있다. 한국의 공인인증서 제도 역시 공개키 기반구조에 입각한 제도이다. 공개키 기반구조에 입각한 인증서는 서버의 신원을 확인하는데 사용되는 서버인증서와 이용자의 신원을 확인하는데 사용되는 개인인증서로 나누어 볼 수 있다. 한국의 공인인증서도 이 두가지 용도에 모두 사용될 수는

있지만, 한국의 공인인증서를 서버인증서로 사용할 경우, 파이어폭스 웹브라우저는 그러한 서버인증서를 신뢰하지 않으므로 현실적으로 서버 신원 확인 용도로 한국의 공인인증기관이 발급한 서버인증서를 사용하기는 무리가 따른다. 한국의 공인인증서는 따라서 개인인증서로 주로 사용되고 있다. 한국의 공인인증서 및 개인키 역시 파일 양식 자체는 국제표준을 따르고 있긴하지만, 그 파일들이 보관, 저장되는 위치와 방법이 독특하여 웹브라우저로는 사용이 불가능하다. 그 결과, 한국의 공인인증서를 이용하려면 이용자가 추가프로그램을 반드시 설치해야만 한다.
인증서는 원래 금융거래에만 사용되는 것이 아니라, 모든 전자적 거래(금전적이건 비금전적이건)에서 당사자의 신원을 확인하거나, 전자서명을 하는 용도로 사용될 수 있고, 한국의 공인인증서도 물론 그런 다양한 용도로 사용될 수 있긴하다. 그러나 현실적으로 공인인증서는 전자금융거래에서 주로 사용되고 있다. 금융위원회는 전자금융거래에 "공인인증서 등"을 사용하도록 강제하고 있다.국내의 경우 사용자가 본인 인증을 받다보니 은행은 손쉽게 해커 유무를 판독할 수 있지만, 사용자는 은행 홈페이지가 진짜인지 피싱 사이트(진짜 홈페이지인것처럼 위장한 해킹 사이트)인지 구분하기 힘들다. 2000년대말 온갖 피싱 사이트가 기승을 부린 이유다. 결국 문제를 깨달은 국내 은행들은 국민은행을 필두로 하나둘씩 자사 홈페이지를 제3자 인증받았다. 공인인증서의 본인 인증방식에 문제가 있음을 스스로 시인한 셈이다.
박 대통령이 말한 무역장벽도 이 공인인증서의 사용자 본인 인증 때문에 발생한다. 국내 사용자의 경우 시중 은행이 본인 인증을 대행하고 있기 때문에 (번거롭지만) 1시간 정도만 투자하면 공인인증서를 발급받을 수 있다. 반면 외국인은 얼마 존재하지도 않는 대한민국 재외공관에 방문해 발급받아야 한다. 땅덩이가 넓은 중국이나 미국같은 나라에선 사실상 불가능한 일이다.
사실 더 큰 문제는 따로 있다. 공인인증서가 보안이라는 원래의 목적에서 벗어나 금융기관의 책임 면피용으로 사용되고 있다는 점이다. 여기선 고려대학교 법학전문대학원 김기창 교수의 발언을 인용한다.
"공인인증서는 정부가 금융기관에게 준 면죄부입니다. 나(금융기관)는 이만큼 보안에 노력을 기울였으니 금융사고가 발생해도 사용자에게 책임을 지지 않는다는 보증서죠. 예를 들어봅시다. 해커가 사용자의 계정과 공인인증서를 탈취해 외국에서 인터넷뱅킹을 시도했습니다. 은행은 단번에 이 사실을 알 수 있죠. 평소에 사용자가 접속하던 국내 IP가 아니라 해외 IP이니까요. 외국 은행같으면 의심스럽기 때문에 이 거래를 거절하고, 즉시 사용자에게 연락을 취할겁니다. 그런데 국내 은행은 그냥 승인합니다. 인증된 사용자(공인인증서)가 거래를 한 것이니 거절할 이유가 없다는 겁니다. 이 때문에 은행의 관리책임을 물어 사용자에게 배상하라는 법원 판결 자체가 나오질 않습니다. 공인인증서가 인감도장과 같은 역할을 하니, 해커가 한 거래조차 사용자가 한 거래로 인식할 합당한 이유가 은행에게 있다는 겁니다. 과거 오프라인상에서나 통할 법할 논리를 21세기 온라인상에서 펼치고 있어요. 이렇게 정부가 면죄부를 발행해주니 은행들은 보안을 강화할 필요성 자체를 느끼지 못하게 됩니다."
국내의 경우 은행 ID/비밀번호, 공인인증서, OTP라는 삼중 보안을 취하고 있다. 반면 해외의 경우 은행 ID/비밀번호, OTP라는 이중 보안을 기본으로 한다. 얼핏 보면 국내가 훨씬 안전할 것 같지만, 실상은 그렇지 않다. 외국 은행의 경우 ID/비밀번호, OTP 외에 참신하면서도 강력한 보안방법을 개발해 자체 적용하고 있다. 뱅크오브아메리카(BOA)의 예를 들어보자. BOA 홈페이지에서 인터넷뱅킹을 하려면 은행 ID/비밀번호, OTP 외에 이미지 패스워드라는 독특한 과정을 하나 더 거쳐야 한다. 사용자만 알 수 있는 암호화된 그림을 보여줘 해당 그림을 찾지 못하면 거래를 진행할 수 없다. 제3자인 해커는 이 이미지 패스워드 과정을 뚫기 힘들다. 외국 은행 대부분이 이렇게 자체 개발한 보안 방식을 적용해 삼중, 사중 보안을 취하고 있다. 반면 국내 은행은 정부가 지정해준 공인인증서에만 보안을 기대고 있다.
미래창조과학부 최문기 장관은 24일 취임 1주년을 맞아 기자들과 만나 액티브X 프리(Free)를 실천해 어떤 웹 브라우저에서도 공인인증서를 사용할 수 있도록 하겠다고 밝혔다. 슬픈 얘기다. 공인인증서에 적용된 암호화 기술 'SEED'는 W3C가 인증한 웹 표준 기술이 아니기 때문에 웹 브라우저 적용하려면 반드시 플러그인이 필요하다. 대안인 HTML5도 원래 액티브X, NPAPI 대체보다 플래시, 실버라이트 같은 액션 스크립트 대체를 목적으로 개발된 기술이다. 웹 표준인 SSL과 EV SSL 인증서가 아닌 다른 보안방식을 쓰려면 결국 HTML5에 확장 기능을 추가해야 한다. 달라지는 게 하나도 없다. 사용자는 여전히 웹 브라우저에 무엇인가를 덕지덕지 설치해야 하고, 은행은 여전히 공인인증서만 철석같이 믿고 있겠다. 외국인은 여전히 국내 쇼핑몰을 이용할 수 없다. 아니면 대한민국판 '천리마 쇼핑몰'을 이용하는 촌극이 벌어지던가.

내의견: 전 레포트에서도 언급했드시 한국 초기에 상황일때는 ActiveX가 필요했다고 생각한다. 하지만 더 좋은 보안성을 가진 프로그램이 나왔는데도 불구하고 그걸 받아드리지 않고 법으로 까지 규제했는지 의문이다. 분명 더 좋은 방법이 있지만 그걸알고도 회피하는 거같다. 공권력과 보안업체간의 뭔가가 있는거같다.
공인인증서는 보안목적으로 만들어졌는데도 불구하고 안전하지않으면서 불편함만 있는거같다 또한 한류등 전자상거래등 산업발전을 막고있는거같다. 그리고 공인인증서를 개인이 너무 보안상태가 안좋은 use나 드라이브등등에 보관함으로써 많은 공인인증서가 유출된거같다. 어서빨리 보안업체와 정부가나서서 해결방안을 찾고 추진해야 한다고 생각한다.