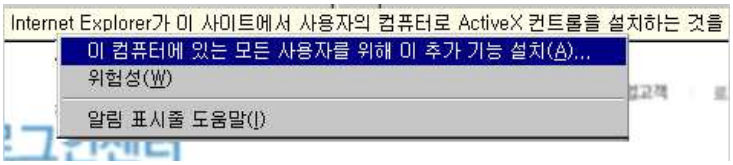
어 ㅅ...*

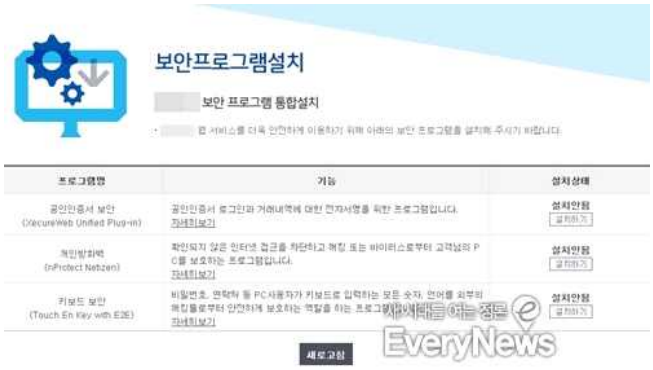
국제표준을 지키지 않는 우리나라의 보안

논산대건고 2616 박성호

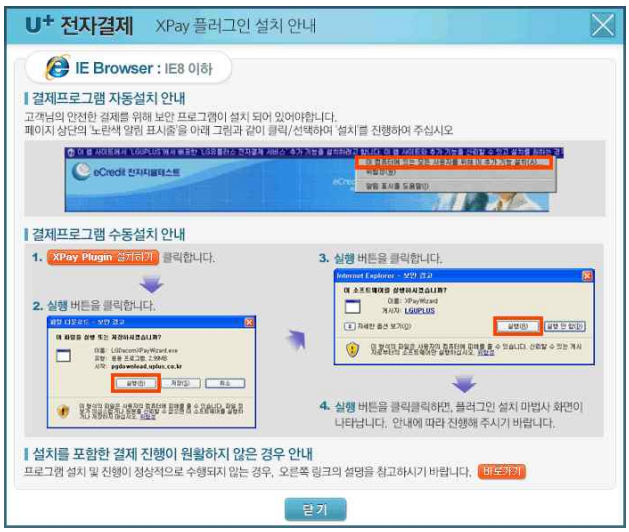
나 강병관(2601). 큰 맘을 먹고 70만원을 들이고 노트북을 인터넷으로 구매하기로 결정했다. 룰루랄라~~. 침을 삼키며 조심스레 결제 버튼을 누른다.



(자연스럽게 설치 버튼을 누른다.)



깔을 게 이렇게 많나? 무조건 깔아야 되는 건가. 좋아. 깔아주겠어. 이건 또 머야?! 바이러스? 백신을 설치하라니 해야겠지. 본격적으로 결제를 진행해볼까.



왜 이렇게 설치하라는 게 많은 거야. 그래도 노트북을 사기 위해서는 모두 설치해야지.

이젠 다 설치했으니 결제를 할 수 있겠지?

으... 언제까지 결제는 안하고 이런 것만 하는 거야. 얼마 전에 4천원 주고 만든 공인인증서를 쓰면 되겠지. 공인인증서 비밀번호가 뭐였지? 네이버 비번이랑 똑같은 거겠지.

(비밀번호를 입력한다) 역시 똑같은 거였네. 드디어 내 노트북이 생겼다!

대한민국에서 결제를 해본 사람이라면 누구나 겪었을 만한 평범한 고등학생의 일화이다. 복잡하고 귀찮은 절차에 자연스레 욕이 나오기도 한다. 우리는 왜 전자결제를 위해서 이처럼 복잡한 절차를 겪어야 하는 것인가? 지금부터 하나하나 알아보자.

1. 왜 이렇게 많은 절차가 필요해?

금융감독원, 보안업계, 은행사 등 관련 기관들이 대답은 간단하다. 그것이 안전한 방법이기에 복잡한 절차가 필요하고 불편을 감수해야 한다는 것이다. 병관이가 설치한 공인인증서 보안 프로그램, 방화벽, 키보드 보안 프로그램, 개별적으로 제공되는 백신, 결제 프로그램을 살펴보면 모두 보안적 절차의 안정성을 확보해 줄 프로그램으로 보인다. 그럼 관련 기관들이 말이 맞는 것이고 우리는 불편을 감수해야하는 것인지 알아보자.

2. 그 전에 하는 SSL 이야기

사실 병관이가 겪은 것과 같은 복잡한 절차는 해외 웹 사이트에서는 찾아볼 수가 없다. 해외 웹 사이트에서 요구하는 것은 신용카드와 주문자에 대한 필수적인 정보이다. 그렇다면 국내에서는 병관이와 같이 복잡한 절차를 거쳐야만 결제 방식을 해외에서는 어떻게 간단하게 진행 할 수 있을까?

그것은 국제표준보안방식인 SSL(Secure Socket Layer)을 사용하기 때문이다. 포털사이트에 로그인을 진행하는 페이지들이 주소는 자물쇠 모양의 아이콘과 함께 https로 시작하는데 이것이 SSL이다. SSL이 어떻게 구현되는지 알아보자.

1. 웹 사이트들은 자신의 안전함을 인증해 보안적 절차의 안정성을 인증받기 위해 국제적으로 관리되는 인증기관들이 제공하는 인증서를 확보한다.
2. 사용자들은 웹 브라우저에서 제공하는 인증기관들의 인증서 검증 기능을 사용해 인증서의 진위 여부를 확인한다.
3. 검증 기능을 통해 검증이 완료되면 미리 약속된 방식으로 보안통신이 시작된다.

사용자와 웹 사이트, 양자의 신뢰성이 확보된 보안통신을 위해서 웹 사이트들은 자신이 안전하다는 것을 인증하는 것이 SSL의 중요한 점이고 한국식 보안 통신과의 가장 큰 차별점이다. 국제적으로 검증된 인증기관들은 피싱 사이트와 같은 불법성이 판단되는 웹 사이트들을 엄격히 판별해 인증서를 발급한다. 국제표준방식이기 때문에 작은 보안결함이라도 발생한다면 거의 곧바로 결함에 대한 보완이 이루어진다. 또한 공개키 암호화 방식의 결함을 보완한 방식으로 이루어지는 보안 통신 덕분에 보안 체계가 상당히 안전하고 전 세계적으로 사용하고 있는 방식이다.

자물쇠가 주소창에 있는지 확인해보자.

결정적으로 사용자가 해야 할 일은 검증기능을 가진 웹 브라우저를 사용해 인증서의 진위를 확인하는 것이고 거의 모든 웹 브라우저들은 검증기능을 보유하고 있기 때문에 사실상 사용자가 할 일은 주소창에 자물쇠 모양이 뜨는지 확인만 하면 된다. 즉, 한국과 같이 프로그램의 설치를 일절 요구하지 않는다.

3. 다시 한국 이야기

결론은 한국은 SSL은 사용하지 않는다. SSL이 웹 사이트가 자신의 신뢰성을 사용자에게 확인시켜 주는 것이라면, 한국은 웹 사이트들이 사용자를 잠재적 범죄자로 인식하고 사용자들은 스스로가 자신이 안전하다는 것을 밝혀야한다. 웹 사이트들은 자신이 안전하다는 것을 밝혀줄 의무가 없다. 다시 말해 사용자들은 웹 사이트들에 대해 신뢰성을 확보할 수가 없다. 웹 사이트의 모든 주소를 외우고 다니지 않는 이상 사용자들은 웹 사이트의 진위 여부를 판별할 수 없다.

웹 사이트의 진위 여부를 확실히 한다면 보안 프로그램들의 설치를 강제하는 한국식 보안 체계가 SSL보다 더 안전하다고 생각할 수 도 있다. 하지만 보안 프로그램을 다운 받는 방식으로는 웹 사이트와의 통신 과정에서 결코 안전을 보장할 수가 없다. 왜냐하면 웹 사이트의 안정성 여부가 확보되지 않았기에, 강제로 설치를 요구하는 프로그램들 사이에 얼마든지 크래커가 원하는 기능을 하는 프로그램이 끼어 올수도 있다. 사용자는 은행 혹은 쇼핑몰에서의 전자 거래를 위해서는 자신의 PC에 어떤 프로그램이 설치되는지 선택할 권한이 없기 때문에 크래커의 프로그램은 너무나도 쉽게 사용자의 PC에 침투할 수 있다. 또한 보안 프로그램 자체의 결함으로 인한 문제보다는 웹에서 이루어지는 불확실한 통신으로 인해 생기는 스니핑의 위험은 얼마든지 일어날 수 있다.

정리하면 한국의 보안 방식은 '서버개방, 사용자 구속'의 체제이다. 그리고 이것이 사용자들을 복잡한 절차 속으로 밀어 넣는다.

4. 구체적인 두 가지 이야기, 액티브 X와 공인인증서

¿ 액티브 X

액티브 X가 문제가 된 것은 오래 전부터이다. MS(Microsoft)도 액티브 X를 버린 지 오래된 이야기이고 대선공약으로 액티브 X를 쓰지 않겠다는 말이 나온 것도 몇 년 전 일이다. 오래 전부터 문제점으로 꾸준히 지목되던 액티브 X가 어떤 것이기에 이처럼 말이 많을까.

가상머신을 통해 다채로운 웹 페이지를 만들게 해주는 자바에 대응하기 위해서 PC에 직접 접근이 가능하게 만들어 자바보다 더 다채로운 웹 페이지를 만들고자 한 것이 MS의 액티브 X이다. 별 문제 없어 보이는 선의의 경쟁으로 보이지만 액티브 X는 보안을 포기한 MS의 대응이었다.

인터넷에서 다운받은 프로그램은 실행 시 백신, 방화벽 등 여러 보안 체제의 감시를 받지만 액티브 X는 인터넷 프로그램이 직접 PC의 자원에 접근하는 것이기 때문에 보안 절차를 일부 무시할 수 있다. 이는 보안적 절차에 심각한 결함으로 직결되지만 PC 자원을 바로 사용한다는 이점 때문에 상당히 널리 퍼지게 되었다. 보안성에 대한 문제가 제기되면서 MS의 제품을 제외한 거의 모든 프로그램들은 액티브 X의 사용을 거부했지만 압도적인 MS의 한국에서의 점유율 덕분에 한국에는 여전히 액티브 X 사용되었다. 문제가 심각해지자 MS조차도 버린 액티브 X는 관리의 이점이라는 명목으로 여전히 한국에 남아있다.

여담으로 한국에서 액티브 X의 존재 때문에 HTML5와 같이 자바와 플래쉬에 대응하는 웹 표준의 바람이 한국에서는 유달리 약했던 이유가 되었고 스마트폰이 급격히 확산되기 시작하자 모바일에서 심각한 호환성 문제로 이어졌다.

MS의 유산이 한국 IT 산업의 발목을 부둥켜 잡고 위협하고 있다. 하지만 이런 상황은 변화를 거부한 관련 기관들 스스로 초래한 것이다.

¿ 공인인증서

나 강병관. 노트북을 사기 위해 70만원과 배송비를 지불한 건 당연해. 그런데 왜 공인인증서가 매년 4천원씩 나가는지 이해가 가지 않아. 1년에 4천원이면 나한테는 아무것도 아닌 돈이기는 하지만 어쨌든 '돈'이 내 통장에서 빠져나가는 것이 이해가 안 된다고!

병관이를 이해시켜주기 전에 SSL 이야기를 다시 해야겠다. SSL은 공개키 암호화 기법에 인증과

정을 추가시킨 것일 뿐 공개키와 개인키를 구분시킨 것은 기존의 공개키 암호화 기법과 같다. 이 때 키의 관리를 서버가 해주기 때문에 사용자는 인증서를 가진 웹 사이트에 접속만 하면 안전한 보안통신이 시작되는 것이다.
한국의 공인인증서도 공개키 암호화 기법을 사용하지만 개인키의 안전이 보장되어야 하는 공개키 기법의 핵심을 무시했다. 공인인증서를 사용해봤다면 C 드라이브의 NPKI라는 폴더에 공인인증서와 키 파일이 존재한다는 것을 알 것이다. 이 키 파일들은 복사를 하는데 전혀 지장이 없기에 누가 언제 복사해가도 알 도리가 없다. 그래서 크래커들이 해킹 프로그램으로 가장 먼저 하는 일이 NPKI 폴더를 검색해 해커에게 전송시키는 것이다. 비밀번호가 걸려 있다 할지언정 크래커들에게 공인인증서 비밀번호를 뚫는 것은 식은 죽 먹기이다.

국내 주요 개인정보 유출사고		
시기	유출 기업	유출 규모
2006년~2008년	하나로텔레콤	650만명
2008년 2월	옥션	1863만명
2008년 9월	GS칼텍스	1119만명
2010년 3월	신세계몰	330만명
2011년 4월	현대캐피탈	175만명
2011년 7월	SK커뮤니케이션즈	3500만명
2011년 11월	넥슨	1320만명
2012년 4월	EBS	400만명
2012년 7월	KT	870만명

3개 카드사의 1억 4000만 건의 개인정보 유출까지 포함시키면 약 2억 4000만 건의 개인정보 유출이 일어났다.

하나 혹은 두 개의 비밀번호만을 사용하는 사용자들의 특성상 위의 표와 2014년의 3개 카드사 개인정보 유출 사고만을 기준으로 전 국민의 개인정보가 4.8회 유출되었다고 생각하면 비밀번호를 알아내는 것은 그리 어려운 일이 아니다.

가장 안전한 비밀번호 방식인 OTP

외국에서는 위와 같이 개인이 설정한 비밀번호의 문제점의 위험도를 인지해 현재까지 제시된 가장 안전한 비밀번호 방식인 OTP를 도입해 사용하고 있다. 우리나라도 OTP를 사용하기는 하지만 공인인증서에서는 사용되지 않고 일부 고액 금융 거래에서만 사용될 뿐이다.

이런 점 때문에 한국식 보안 체계가 SSL과 같은 방식의 암호화 기법을 사용하지만 현실적으로는 상당히 취약한 이유이다. 관련 정부 기관들은 기술력이 부족해서 안전한 키의 저장을 실현시키지 못한 것도 아니다. 거의 모든 사람들이 사용하는 운영체제인 윈도우즈, 리눅스, 매킨

토시는 무료로 안전성이 보장된 키 보관 저장소를 제공해준다. 무료로 제공해주는 안전한 저장소가 있는데도 사용하지 않는 것이다.

공인인증서 발급 업체

이런 문제점 뿐인 공인인증서를 아직도 사용하는 이유는 금융감독원과 보안 업체의 이윤 때문이다. 공인인증서는 매년 일반 사용자에게는 4천원을, 사업자에게는 1만원을 받는다. 또한 폐쇄적인 보안정책에서 그들은 보안업계에서 권위를 지닐 수가 있다.
또 다른 이유로는 '공인인증서는 키 관리는 제외하고는 SSL보다 훨씬 안전하다' 혹은 'SSL도 해킹당하는데'라는 일부 관계자들의 망언이다. 키 관리에 대해서 이야기하면 보안 체계에서 단 하나라도 결함이 존재하는 절차가 발견된다면 그 보안 체계는 안전하지 않은 보안 체계로 평가 받기 때문에 키 관리를 제외하고 안정성을 논할 수는 없다. 또한 SSL도 해킹사고가 일어난다. 하지만 대부분 서버에서 개인키가 유출된 것이다. 서버에서 유출되었기에 개인 사용자와는 다르게 키가 유출됐다는 사실을 관리자는 인지할 수 있고 즉시 해킹당한 키의 인증서 폐지, 새로운 인증서 발급, 웹 브라우저들에게 사건 통지가 이루어진다. 이는 국제적인 뉴스거리가 될 만큼 드물게 일어난다. 오히려 공인인증업체, 은행, 금융감독원, 금융결제원 등 관련 기관들은 대부분의 사건들에 대해서 쉬쉬하며 넘어가는 것이 다반사다.

병관이가 불편하게 공인인증서를 사용하면서 돈을 지불한 까닭은 결국 관련 기관의 이득과 망언 때문이었던 것이다.

5. 마치며

한국식 보안 체계를 폐지하고 국제표준보안방식(SSL)을 모든 안전한 통신이 요구되는 범위에서 도입해야 한다. 사용자들은 스스로 자신의 보안을 구축해야하고 웹 사이트들은 이를 강제하지 말아야한다. 컴퓨터를 잘 모르는 사람들을 위해 기본적인 보안 가이드라인을 제시해 줄 수는 있지만 선택사항으로 남겨 둬야 한다. 기존에 사용하던 OTP는 범위를 확대해야한다. 또한 관련기관들의 개혁 의지를 관철시키기 위해서는 많은 국민들이 이런 잘못된 보안 업계의 사실을 깨닫고 불만을 가지고 목소리를 내야 한다. 결국은 국민들 스스로가 문제점을 파악해야 국민들의 안전이 보장되는 길이 생기는 것이다.