2차과제 / 한아름

HTTP와 HTTPS는 무엇이며 그 차이는?

HTTP(HyperText Transfer Protocol)

- 월드 와이드 웹 상에서 정보를 주고받을 수 있는 프로토콜.
- 주로 HTML 문서를 주고받는 데에 쓰인다.
- HTTP는 클라이언트와 서버 사이에 이루어지는 요청/응답(request/response) 프로토콜이다.

HTTPS(Hypertext Transfer Protocol over Secure Socket Layer)

- 월드 와이드 웹 통신 프로토콜인 HTTP의 보안이 강화된 버전.
- HTTPS는 통신의 인증과 암호화를 위해 넷스케이프사가 개발했으며, 전자 상거래에서 널리 쓰인다.
- HTTPS는 소켓 통신에서 일반 텍스트를 이용하는 대신에, SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화한다.
- HTTPS에서는 데이터를 전달할 때 공개키와 비밀키에 기반한 암호화를 거치므로 사용자의 데이터를 안전하게 숨겨준다.

왜 보안에 더 특화 된 HTTPS를 쓰지 않는 것 인가?

1. 캐시를 하지 못함

2. 성능문제
SSL의 이니셜키 교환은 호출 시간을 더 들여야 함. 순수한 보안의 목적을 위해 HTTPS 전용 웹을 사용할 경우, 오늘날의 기술을 가지고 서는 속도가 느려질 수 있다. 또한 로그인을 하지 않는, 암호화를 할 이유가 없는 사이트라면 HTTPS는 합리적이지 못하다.

3. 비용 문제
HTTPS 사이트를 돌리는 데에는 비용이 더 많이 든다. SSL을 더 최적화시켜서 구현하는 등, 서버가 더 빨라질 수는 있지만, 그래도 단순한 HTTP보다는 비용이 더 많이 들어간다. 트래픽이 거의 없는 작은 사이트에서야 별 문제가 되지 않지만 사이트가 갑자기 유명세를 탈 경우 HTTPS는 비용 문제를 일으킬 수 있다.

4. 가상 호스트와의 호환 문제
저렴한 웹 호스팅이 제공하는 가상 호스트는 동일한 물리적 서버에서 다중의 웹사이트를 서브할 수 있게 해 준다. 즉, 수 백 가지의 웹사이트가 동일한 IP 주소를 사용하는 것. 보통의 HTTP라면 괜찮겠지만, 이 경우 HTTPS와는 전혀 잘 돌아가지 않는다.

국내에 공인인증서가 생긴 배경과 그 위험성

**** 공인인증서란?**
- 대한민국에서 인터넷을 이용하여 금전거래를 할 때 인증을 위해 필요한 전자서명. 일종의 컴퓨터 파일.
- 전자상거래시 본인만 해당 인증서를 갖고 있고, 본인만 인증서 비밀번호를 알기 때문에 본인임을 인증할 수 있는 전자서명으로 이용 가능.

국내에 공인인증서가 생긴 배경 - > 정부 주도 하에 특정 기술의 사용 의무화

정보통신부가 존재하던 시절 정통부의 고민은 새로운 먹거리 창출이였다. 그래서 정보통신부는 보안 분야로 눈을 돌리게 되었다. 하지만 보안분야, 그 중에서도 특히 암호 관련 분야는 국가정보원이 있었기에 정통부가 끼어들 틈이 없었다. 이 때 정통부가 내세운 논리가 전자서명을 위한 인증체계 구축이였다. 전자서명을 위한 인증체계 구축은 인터넷 상에서 전자상거래를 하기 위해서는 전자적인 형태의 인감도장과 인감증명서가 필요한데, 이러한 전자 인감도장과 전자 인감증명서 발급체계를 정통부가 주도하여 구축하겠다는 것을 의미한다. 전자서명인증체계의 주도권을 쥔 정통부는 몇 가지 이유로 무리한 계획을 세우기 시작했고 공인인증서 1,000만개 보급 운동 이라는 재앙이 시작되게 되었다.

도장에도 막도장과 인감도장이 있듯이 PKI에도 개인(또는 일반회사)이 구축한 사설 PKI와 국가가 구축한 공인 PKI가 있다.
이때 사설 PKI를 통해 발급된 증명서를 '사설인증서'라 하고, 공인 PKI를 통해 발급된 인감증명서를 '공인인증서'라고 한다.
당시만해도 일부 업체와 은행에서는 사설인증서를 이미 인터넷 계좌이체 등의 업무에 활용하고 있었으나 정보통신부가 무리하게 공인인증서 1,000만개 보급운동을 전개하면서 은연중에 사설인증서는 공인인증서에 비해 안전하지 못하다는 인식이 퍼졌고, 그 결과 우리나라에서 사설인증서는 거의 자취를 감추게 되었다.
**사설인증서나 공인인증서나 발급의 주체가 개인(또는 회사)이냐 국가냐의 차이이지 사실 사용하는 기술은 같다.

공인 인증서의 위험성

• NPKI 폴더라는 비표준적 위치에 저장되고 있으므로, 사용자들이 별도 프로그램을 컴퓨터에 설치 해야하는 번거로움과 보안상의 위험이 따른다.
• 단순히 copy & paste 함으로써 이용자의 인증서 개인키가 쉽게 복제, 유출될 수 있다.
• 다양한 운영체제이나 디바이스, N-스크린 환경에 대응하기가 어렵다.
• 글로벌 표준과 동떨어진, 고립된 인터넷 환경을 조성하고 있다.
• 공인 인증서의 유출로 인한 보이스피싱이나 피싱·해킹 등의 금융사고 피해가 다수 발생하고 있다.

위의 내용을 조사하며 느낀점

공인인증 제도, 공인인증 기술은 보안 업체들이 안전하다는 프로그램을 전 국민의 컴퓨터에 설치해야 구동되는 체제이나 13년이 넘는 긴 시간 동안 한국의 IT는 전 국민의 안전, 대한민국 IT의 안전 문제에 관해 3~4개의 보안 업체 말만 믿고 굴러 왔다고 해도 과언이 아니라고 한다. 국가와 기업에 의해 강제된 기술은 무능해졌을 뿐 아니라 해결 하기도 어려운 골칫덩이가 되어 버렸다. 장기적인 플랜과 대안책 마련 없이 주먹구구식으로 처리하는 정부의 안일한 행정처리 방식은 국민들에게 또 다시 화살이 되어 날아와 버렸다. 과연 한국은 다시 한 번 IT강국이 될 수 있을까? 기술로 살아남고 경쟁력을 갖추는 국가가 될 수 있을까? 답답함과 안타까움만 공존하는 현 상황이 아쉽기만 하다. 정부와 기업 그리고 민간 전문가들의 협업을 통해 문제에 대해 다시 한 번 올바르게 직시하고 IT산업과 첨단산업에 대한 규제를 좀 더 체계적이고 미래지향적으로 개선하고 발전 시켜 나갈 수 있는 체제가 조속히 마련되었으면 한다.