과제

개요
1. http/ https 이 둘의 차이는?
2. 공인인증서 생긴 배경과 그 위험성
3. 위의 내용을 조사하며 느낀점

1. http/ https 이 둘의 차이는?

http

Hyper Text Transfer Protocol
Hyper Text를 전송하기 위한 프로토콜
(프로토콜(protocol): 통신 프로토콜 또는 통신 규약이라 불린다. 컴퓨터를 포함한 원거리 통신장비 사이에서 메세지를 송수신할때 정해진 양식과 규칙이다. 국제전화가 가능한 것도 이러한 프로토콜을 준수했기 때문이다.
통신할때의 약속이라고 생각하면 간단하다)

Http의 구조는 Request와 Response로 구성되어있다. 우리가 사용하는 웹페이지 www앞에 http:// 가 붙어있다는 것은 http 프로토콜로 통신하겠다는 뜻이다.
<form method="[ ] "> 태그의 [ ] 안에 들어가는 post, get방식이 바로 http통신 방법이다. get방식을 예로들면 yagom.net/page=1 을 서버에 보냈을때 서버에서 yagom 블로그의 1페이지를 보여달라는 뜻이다. 이러한 통신을 주고받을때 송신, 수신 양쪽의 약속이 http이다.

https

https는 http + security 보안이 들어갔다는 뜻이다.
개인정보법안이 강화 되면서 개인정보를 송수신할땐 반드시 https 프로토콜을 사용해야 한다. 이것이 지켜지지 않을경우 해당 사이트 업주는 벌금을 물거나 해당 신고가 누적되었을때 사업 중지에 처하기도 한다.
하지만 그럼에도 불구하고 아직도 수 많은 사이트는 그냥 http를 사용한다.

cafe24에서 http://www.cafe24.com/?controller=product_page&type=vservice&page=ssl 보안서버 구축 의무화 라고 하여 이 인증서를 구매하여 내 서버에 설치할 수 있다.

url링크에서 보면 page=ssl로 나와있듯이 흔히 ssl(Secure Sockets Layers)로 알고있지만 정확한 명칭은 TLS(Transport Layer Security)이다.

위의 http의 form태그를 설명하였는데 action속성에 blog.yagom.net이 ssl 인증서를 사용한다면
<form action="http://blog.yagom.net:443"> 으로 명시한다 (443 포트를 통해 데이터를 전송함. - 이건 어디까지나 디폴드 환경이고 이것을 구축한 사람이 다른 포트를 사용한다면 포트가 바뀔것이다.)

온라인 사이트에서 결제를 할때 고객은 그 사이트가 피싱사이트는 아닌지 확인할 수 있어야 하며, 해당 사이트는 자신의 고객이 맞는지 확인해야하는 의무가 있다. 그리고 주고받은 데이터는 제 3자에 의해 도청되지 않도록 암호화하여 통신해야하는데 이럴때 사용하는게 TLS 즉 https 통신이다.
cafe24에서 가격에 차이를 두고 있는데 128bit암호화 혹은 256bit 암호화를 사용하여 데이터를 주고받는다(주고받는 데이터는 로그인 아이디, 패스워드가 포함이다.)

내가 해본적은 없지만 전송하는 패킷을 스니핑이라는 과정을 통해서 얼마든지 감시할 수 있다고 한다.
아이디와 패스워드가 암호화되지 않고 제 3자에게 틀킨다면 그것이 어떻게 사용될까?
요즘 스마트폰과 컴퓨터를 보면 그 사람이 어떤것에 취향이 있고 무슨생각을 하는지, 좀 더 전문적인 사람들은 그 사람의 심리상태까지 측정할 수 있다고 한다. 바로 이러한 치명적인 정보들이 그냥 누출되는 것이다.

그렇다면 ssl 인증서를 사용해서 암호화된 데이터를 사용할 경우 어떠한 과정을 거치게 될까?
실제로 데이터를 주고받기 전에 Handshake(악수)라는 과정을 거치는데 내용은 다음과 같다.

1. 클라이언트가 서버에 접속한다(Client Hello) 이때 아래 데이터가 함께 송신된다.
    1. 클라이언트측에서 생성한 데이터(CA)
    2. 클라이언트가 지원하는 암호화 방식

3. session ID: 이전에 이 사이트에 해당 사용자가 접속하여 통신을 했었다면 리소스를 절약하기 위해 기존의 세션을 재활용한다. 이 때 사용할 연결에 대한 내용을 서버로 전송한다.

2. 서버는 응답으로 Server Hello를 한다. 이때 응답 내용은 아래와 같다.
   1. 서버측에서 생성한 데이터(CA)
   2. 서버측의 암호화 방식
   3. 인증서

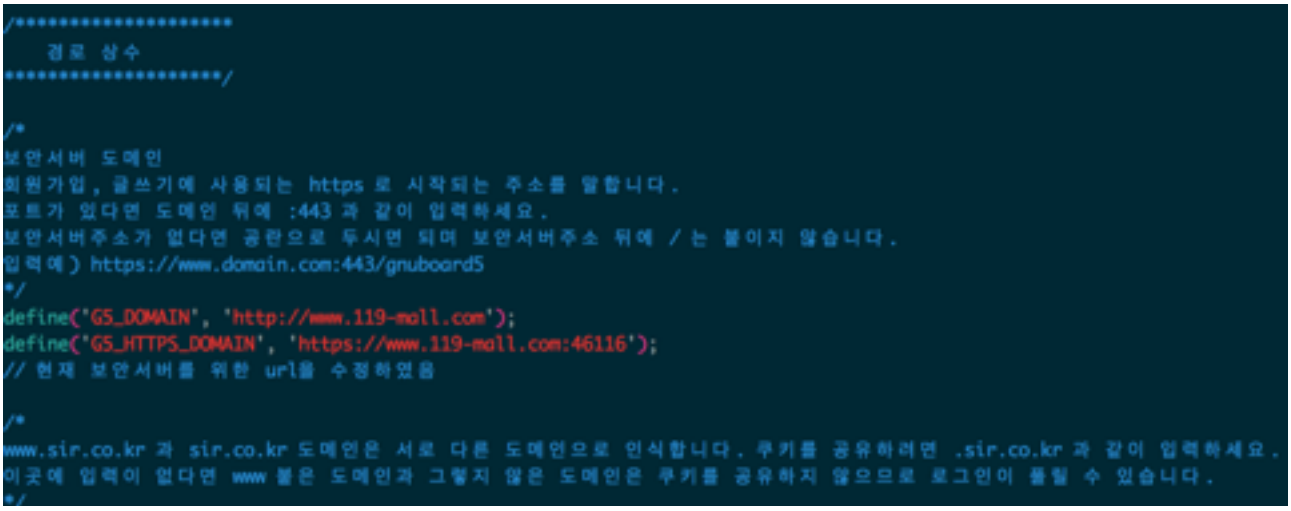
3. 클라이언트는 서버의 인증서가 CA(Certificate: 검증기관)에 의해서 발급된 것인지 확인하기 위해 CA 리스트를 확인한다. 해당 리스트에 인증서가 없다면 사용자에게 경고메세지를 전송한다. 확인 과정은 클라이언트에 내장된 CA의 공개키를 이용해 복호화를 하는데 성공하면 인증이 된것이다. 서버측에서 생성한 데이터와 클라이언트가 생성한 데이터를 조합해 pre master secret 이라는 키를 생성한다. 이 키가 서버와 클라이언트가 데이터를 주고받을때 송수신한 암호화한 데이터를 복호화하는데 사용한다. 이 키값은 제 3자에게 노출되어서는 안된다. 그리고 이 pre master secret은 서버로 전송된다.

4. 서버는 클라이언트가 전송한 pre master secret 값을 자신의 비공개키로 복호화한다. 그리고 서버와 클라이언트 모두 pre master secret을 master secret으로 만든다. 이 master secret은 session key를 생성하는데 이 session key값을 서버와 클라이언트가 공유한다. 이 값으로 서버와 클라이언트가 암호화한 데이터를 주고받아 복호화한다.

5. 클라이언트와 서버는 핸드쉐이크 단계의 종료를 서로에게 알린다.

요즘의 웹 트랜드는 경량화인데 이렇게 암호화된 데이터를 주고받으면 굉장히 큰 패킷을 주고받게 된다. 하지만 보안을 위해서 반드시 사용해야한다. 해외 사이트는 이러한 상황과 대한민국에 비해 상대적으로 느린 네트워크를 고려하여 사이트를 화려하게 꾸미기보단 이러한 데이터 경량화에 집중한다.
최근 그누보드 youngcart5(https://github.com/gnuboard/youngcart5)

http와 https의 차이는 보안유무이다. 이제 개인정보를 주고받는 모든 사이트에서는 https 통신이 필수이다.



여기 코드를 보면 https 통신을 할 경우에 정의하는 곳이 따로 있다 (config.php)

+CA 인증기관
미국
comodo group(https://www.comodo.com/): 한국 standard chartard 은행이 여기 인증서를 사용하고 cafe24에서 발행하는 ssl 인증서 역시 이곳에서 발행한다.

Geo Truest(https://www.geotrust.com/)

godaddy (http://www.godaddy.com/) 미국에서의 cafe24

Thawte(http://www.thawte.com/): Versign과 함께 CA에서 오래된 회사이다.
우분투를 만드는 캐노니컬을 창립했다.

VerSign(http://www.verisign.com/): 한국에서도 이 인증서가 굉장히 친근할것이다.

대한민국
한국정보인증(http://www.kicassl.com/): 코모도 한국 공식인증 ssl국내 1위
한비로(https://www.comodossl.co.kr/)
카페24(http://www.cafe24.com/)
가비아(https://sslhosting.gabia.com/service/)

2. 공인인증서 생긴 배경과 그 위험성

과제 주제부터가 공인인증서의 단점에 대해 서술하란 내용이다. 내 생각엔 1년에 한번씩 그리고 기기를 포맷하거나 스마트폰 OS업데이트로 삭제시 다시 설정해줘야 하는것, 은행끼리 연동이 쉽지 않아 타행인증서로 등록해야하는 단점을 제외하곤 나름 괜찮다고 생각한다(쓰고보니 다 단점이네?)

역사

1. 1999년 전자서명법 발효이후 상공회의소+행정부 // 금융결제원, 은행, 금융업계 두 파벌로 나뉨
2. 행정부는 모든 국민의 갱니정보를 행정부가 보증하였고 사인 발급은 한국정보인증(KICA, Signgate)가 담당하였다.
3. 금융결제원, 은행, 금융업계는 yessign이 발급 주체가 되었고 이 3업계의 개인정보 보증 주체가 됨
    1. 이 뜻은 금융정보 보증을 국가 혹은 공기업이 아닌 사기업이 주체가 되었다는 뜻이다
    2. 은행권은 금융결제원(yessign)이 보증을 서는 범용 인증서를 만들었다(은행은 사기업이다)

이때만 해도 전자와 관련된 법이 없어서 이렇게 두군데가 나뉘어도 명확한 보안 기준이 없더라도 문제는 없었지만 2001년 전자 정부법이 발효되고, 전 국민이 공인인증서와 부딪히면서 이에대한 반발과 불평이 쏟아져나왔다.
결국 전자서명법이 개정 되었고 정부가 보증을 서게 됨.

누가 그랬다 공인인증서 ActiveX 만든놈은 방안에 가두고 물을 잔뜩 먹인다음 화장실 가고싶을때 문 열려고 하면 ActiveX를 설치하고 공인인증서로 인증시킨다음에 화장실 보내줘야한다고(쉽게 화장실에 가지 못할테니까)

현황, 위험성
공인인증서는 ActiveX가 대한민국 웹에 덕지덕지 발라지게 된 원흉이라고 한다.
쇼핑몰, 은행등에서는 이 인증서가 필수적이다. 하지만 모바일 환경에서는 한번만 제대로 설정을해주면(그 한번이 문제임) 별다른 ID, password 입력없이 인증서로 로그인만 하면되기 때문에 간편하다고 생각한다.

전자정부 시스템에서도 공인인증서를 사용하는데(공무원들이 사용함) 종이문서 공문이 전자문서로 대체되면서 날인이 공인인증서로 대체된것이며, 병무청사이트, 국가 장학금 신청, 자격증 시험 응시, 인터넷 뱅킹등에 사용된다. (위에서 서술함)

공인인증서의 보안이 취약하다 라는 견해가 수 많은 블로거들 사이에 공공연히 퍼져있는데 이건 고려해볼 필요가 있다. 신뢰도가 다소 부족한 정보이지만 신종금융범죄 중 해킹에 의해 암호를 알게되어 발생한 피해건수는 전체에서 1%약간 넘는 수준이라고 한다. 금융정보는 100% 보안이 유지되어야 하지만 페이팔은 3~5% 이다.

그치만 이것은 뭘 모르는 블로거들의 의견이고 이 공인인증서를 해석할 실력있는 크래커의 손에 공인인증서가 들어가면 어떻게 될까? 우리가 아는 모든 사이트가 위험해지는것은 99%의 평범한 인간이 아니라 1%도 안되는 이런 실력자들 때문이다.

이 공인인증서는 hdd나 usb등의 별도 저장장치에 저장해서 소유해야하고 이것을 사용하기위해 별도의 프로그램이 필요한건 사실이다. 그리고 공인인증서를 복사하는것도 간단하다. 해당 폴더를 그냥 복사하면 된다. 나도 맨 처음엔 hdd에 저장을 하고, 이후에 usb로 옮겨가서 내가 사용하는 모든 컴퓨터에 저장해뒀다.

실례로 인터넷 결제를 잘 모르는 나이많은 아줌마가 내 컴퓨터에서 자신의 카드를 이용해 공인인증서를 등록하고(내가 해줌), 카드로 등록해서 결제를 한적이 있었는데 공인인증서는 이미 내 컴퓨터에 설치되어있고 암호 역시 내가 만들어준 상황이다. 그럼 그 아줌마의 카드로 내가 원하는 물건을 결제하는데는 아무런 문제가 없다.
이것은 회사에서도 동일하다. 경리직원이 비밀번호도 알고있는 경우가 많은데 인증서를 복사해가서 엄청나게 많은 것을 결제해버린다면, 이건 답이 없는 상황이다.

3. 느낀점 (https://brunch.co.kr/@jsksoft/20 대한민국 10년뒤 무엇을 먹고살것인가?)

먼저 주변 상황에 대해 좀더 관심과 호기심을 가져야겠다는 생각이 들었다
은행에서 발급받은 인증서와 증권가에서 받은 인증서 두가지가 있는데 이 이유를 이제서야 알게되었다.
심지어 나는 그 발급한 회사가 같은곳인줄 알고있었다.
인증서를 스마트폰에 넣어둔 상태인데 한번 넣는게 귀찮아 차일피일 미루다 6개월이나 지나서 인증서를 설치한게 사실이다. 이론적으로는 나름 편리한 솔루션이라고 생각했지만, 사실적으로 보면 난 공인인증서를 굉장히 귀찮아 한 것이다.

그리고 중요한 사실은 윈도우에서만 사용이 가능하다. 미래창조과학부에서 pkg파일로 공인인증서를 만들어 맥에서도 사용이 가능하겠다는 말을 했다고 하는데 제발 사실이 아니면 좋겠다

학점은행제 사이트 www.cb.or.kr은 크롬브라우저를 지원하는데 특정 버젼만 지원하고 심지어 그 버젼은 이제 구하기도 힘들다. 그래서 결국 윈도우를 켜고 IE에서 필요한 작업을 진행했는데 딱히 맥이라고 다를거같진 않다
게다가 맥은 가상머신위에서 돌아가는 OS가 아니다

그런데 이렇게 불평만 해도 되나 싶은것은 대한민국의 미래이다.
중국의 경우 하드웨어 차이가 매우 심각하다. 아직도 486 컴퓨터를 사용하고 있는 유저가 많다. 그 수가 너무 많기 때문에 개발자들이 IE6에서도의 환경도 고려한다고 하는데 한국은 하드웨어가 너무 뛰어나서 이것을 고려할 이유가 없다. 오히려 IE6에서의 호환을 요구하는 클라이언트를 만났을때 반응은 굉장히 부정적이다. 나 또한 그러했다.

안드로이드 기기만해도 다양한 수요를 갖고있는 중국 개발자들은 불평을 가지면서도 이 부분에 대해 고려하며 프로그램을 만드는데(하지만, 인권이나 노동법은 안드로메다) 한국 개발자는 이러한 훈련이 전혀 안되어있다.

지금 모바일시장(샤오미를 포함해 전세계 측면에서 봤을때 한국은 이미 졌다), 핀테크 사업까지 중국을 상대로 이기는 사업이 별로 없다. 중국인 기획자, 개발자들이 한국인 기획자 개발자를 상대로 아직도 모바일에 감이 없다는 평가를 내렸다고 한다. 어이없지만 cafe24가 알리바바로 부터 들은 답변이다.

웹표준에 최선을 다하기위해 이런 activeX 공인인증서는 없어져야 할 솔루션이지만, 이제 프로그래밍을 배우는 한 사람으로서 과연 불평만 해야할까?