공개 소프트웨어 환경에서의 인터넷 뱅킹 서비스를 위한 PKI 기반 기술에 대한 연구

한명묵* · 이철수*

요 약

국내 인터넷뱅킹 환경은 Microsoft 사의 Internet Explorer(IE) 브라우저에 맞게 구축되어 있어, Linux나 FreeBSD 등과 같은 공개 운영체제 및 웹 브라우저에서는 인터넷뱅킹 서비스를 이용할 수 없었다. 이런 문제 해결을 위해, 본 논문에서는 먼저 SEED를 이용한 공개 소프트웨어 환경에서의 전자 지불 시스템을 위한 전자 서명 시스템을 개발한다. 국내 인터넷뱅킹은 현재 공인인증기관이 발행하는 공인인증서를 통해 인증 및 전자서명 검증이 이루어져야 하는데, 그에 맞춰 공인 인증서 유효성 검증 시스템을 분석 및 개발한다. 마지막으로 자체 개발한 웹 서버에서는 이미 가상 인터넷 뱅킹환경이 구축되어 있어 SEED가 포팅 된 모질라 환경을 가지고 있는 클라이언트에서는 인증서를 설치하여 기본 인터넷뱅킹 서비스를 가상으로 받을 수 있으며 인증서 인증 및 전자서명이 정상적으로 작동되고 있다는 것을 구현을 통해 확인했다.

A Study on the PKI based Technology for Internet Banking Service in the Open Software Environment

Myung-Mook Han* · Chulsoo Lee*

ABSTRACT

Since the domestic internet banking environment has established for Microsoft Internet Explorer (IE), the internet banking service is not able to use in the open operating system and web browser such as linux and freeBSD. To solve the problem, we develop the digital signature system used the seed for the digital payment system in the open software environment. Because the domestic internet banking performs the certificate and digital signature verification through official certificate that the official certificate authority issues, we analyze and develop the verification of validity system for the official certificate. Since the virtual internet banking environment is already established in the web server developing under the self-abilities, the basic internet banking service can be performed installing the certificate in the client which has the mozilla porting the seed. Finally, we can confirm that the certificate and digital signature are performed normally through the experiment.

Key words : Internet Banking, PKI(Public Key Infrastructure), Open Software

* 경원대학교 소프트웨어대학

1. 서 론

IT기술의 발전에서 소프트웨어는 그 핵심을 이루고 있지만 특정 업체의 기술에 기반을 두어 그에 의존적인 환경이 구축되고 있다. 이는 향후 국가 경제나 안보를 위협할 수 있을 정도의 위협이 될 수 있다. 선진국은 이러한 사항을 인식하여 공개소프트웨어 활동을 전개하고 있으며, 국가에 관계없이 공동의 작업을 수행하는 협동 노력을 하고 있다. 즉 미국, 유럽 등 선진국을 중심으로 공개소프트웨어의 중요성이 인식되어 관련 인력을 양성하고 활발한 연구 활동을 하고 있다[1]. 정보사회에서 정보인프라는 그 나라 발전 가능성의 척도가 되고 있다. 우리나라의 초고속 정보통신 인프라가 국제적으로 가장 우수한 것은 세계적으로 인정된 사실이다. 정보보호는 정보통신 인프라와 같이 정보사회의 중요한 인프라에 해당한다. 그럼에도 불구하고 우리나라의 정보보호 환경은 OECD 국가 중에 최하위에 머물고 있는 실정이다. 최근에 와서 정보통신부가 정보보호 환경을 위하여 많은 투자와 노력을 아끼지 않고 있다[2].

현재 국내 인터넷뱅킹 환경은 Microsoft Windows 상에서의 IE(Internet Explorer) 브라우저에 맞게 구축되어 있어, Linux나 FreeBSD 등과 같은 공개 운영체제 및 웹 브라우저에서는 인터넷뱅킹 서비스를 이용할 수 없었다. 이러한 문제는 인터넷뱅킹을 위한 PKI 공인인증 보안 소프트웨어가 Internet Explorer만 지원하도록 만들어져 있고, 은행의 인터넷뱅킹 서비스 컨텐츠가 IE만 지원하도록 만들어져 있어 발생하는 것이다. 따라서 문제해결을 위해, 먼저 공개 소프트웨어 환경에서 사용할 수 있는 PKI 기반 기술 개발이 필요하다[3-5].

이를 위해 본 논문에서는 먼저 SEED를 이용한 암호화 적용이 이루어져야하기 때문에 사용자 웹 브라우저와 웹 서버의 SSL 보안채널에 SEED 알고리즘을 적용하는 작업을 한다. 또한 공개 소프트웨어 환경에서의 전자 지불 시스템을 위한 전자서명 시스템을 개발한다. 국내 인터넷뱅킹은 현재 공인인증기관이 발행하는 공인인증서를 통해 인증 및 전자서명 검증이 이루어져야 하는데, 그에 맞춰 공인 인증서 유효성 검증 시스템을 분석 및 개발한다. 마지막으로 자체 개발한 웹 서버에서는 이미 가상 인터넷 뱅킹환경이 구축되어 있어 SEED가 포팅 된 모질라 환경을 가지고 있는 클라이언트에서는 인증서를 설치하여 기본 인터넷뱅킹 서비스를 가상으로 받을 수 있으며 인증서 인증 및 전자서명이 정상적으로 작동되고 있다는 것을 확인할 수 있다.

본 논문의 구성은 다음과 같다.

2장에서는 인터넷 뱅킹 동향에 대해서 설명하고, 3장에서는 공개 소프트웨어 환경에서의 인터넷 뱅킹 서비스를 위한 PKI 기반 기술에 대한 전반적인 개요를 소개한다. 4장에서는 실제적인 실험 과정과 인터넷 뱅킹 서비스를 구현하고, 마지막으로 5장에서는 결론과 향후 연구과제에 대해서 기술한다.

2. 인터넷 뱅킹 동향

현재 국내 인터넷뱅킹 환경은 Microsoft Windows를 기반으로 한 IE(Internet Explorer) 브라우저에 맞게 구축되어 있어, Linux나 FreeBSD 등과 같은 공개 운영체제 및 웹 브라우저에서는 인터넷뱅킹 서비스를 이용할 수 없다. 이는 인터넷뱅킹을 위한 PKI 공인인증 보안 소프트웨어가 Internet Explorer만 지원하도록 만들어져 있고, 은행의 인터넷뱅킹 서비스 컨텐츠가 IE만 지원하도록 만들어져 있어 발생하는 것이다.

국내 인터넷뱅킹은 현재 공인인증기관이 발행하는 공인인증서를 통해 인증 및 전자서명 검증이 이루어진다. 국내 금융서비스(인터넷뱅킹)는 금융감독원의 보안성 심의 기준에 의거하여 반드시 SEED를 이용한 암호화 적용이 이루어져야 한다. 국외 금융서비스는 SSL v3/TLS v1 기반의 암호

화 방식을 적용하며, 국가 규정에 따라 전자서명을 적용하는 경우도 있다. 국외 금융기관의 국내 인터넷뱅킹 서비스의 경우 현재 국내 공인인증기관이 발행하는 공인인증서를 기반으로 하는 서비스 모델을 금융감독원이 권고하고 있으나, SEED 지원 문제에 대한 결정이 이뤄지지 않은 관계로 인터넷뱅킹 서비스가 활성화 되어 있지 않다.

SSL v3/TLS v1은 Netscape 사가 웹 브라우저와 서버 사이의 보안을 위해 만든 수송계층의 보안 프로토콜로서 대칭키 암호 및 공개키 암호 기법을 이용 클라이언트/서버 사이에 범용적인 보안을 지원하는 구조로 설계되었으며 강력한 서버 인증 기능을 지원하는 프로토콜로 국내 인터넷뱅킹에서는 사용하지 않는다.

전자서명은 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화 방식을 이용하여 전자서명 생성키로 생성한 전자문서(일반적으로 파일 형태)에 대한 작성자의 고유한 정보를 말한다.

PKCS은 PKI 관련 국제적 사실 표준 규격으로 정의된다.

SEED는 정보통신부, 정보보호센터가 민간 부문의 활용을 위해 보급중인 대칭키 암호화 알고리즘으로서 128bit 블록 암호화 알고리즘(128bit Symmetric Block Cipher, SEED). 금융권의 인터넷뱅킹은 반드시 SEED 국가표준 암호 알고리즘을 사용해야 한다.

OCSP(Online Certificate Status Protocol)는 고객이 사용하는 인증서에 대한 유효성을 검증하기 위한 것이며 실시간으로 인증서의 폐기 정보를 조회할 수 있는 기능이 필요한 업무를 위해서 고안된 인증서 상태 조회 프로토콜이다.

CMP(Certificate Management Protocol)는 IETF에서 표준화한 기술로써 인증서를 관리하는 데 사용되는 프로토콜. 인증서 신청, 폐지, 갱신, 변경, 상호 인증 등의 인증서 관리 업무를 처리하도록 구성하는 데에 필수적인 프로토콜이다.

3. PKI 기반 기술 개요

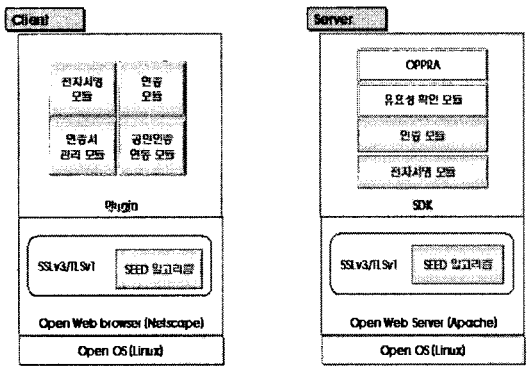
금융서비스를 위한 데이터 암호 알고리즘으로 SEED 국가표준을 사용하여야 하므로 공개소프트웨어 웹 브라우저와 웹 서버에 SEED 암호 알고리즘이 지원되어야 한다. 웹 브라우저에는 응용서비스 데이터에 대한 전자서명 기능이 제공되지 않으므로 금융거래를 위한 데이터에 전자서명을 할 수 있도록 하기 위한 Plug-in 모듈을 개발한다. 국내 6개 공인인증 기관들이 발급하는 공인인증서에 대한 발급/폐기/갱신 기능과 인증서 복사/삭제/형식변환 등의 관리 기능을 제공하는 모듈 개발한다. 웹 브라우저가 서버에 전달하는 전자서명 정보에 대한 검증 역할을 수행하는 서버 모듈이 필요하다. 인터넷뱅킹 환경을 제공하기 위한 사용자 UI가 KISA에서 제정한 표준 규격으로 나와 있으므로 이를 구현하여야 한다.

3.1 WWW 보안을 위한 SSL/TLS

SSL/TLS 전자상거래 보안 프로토콜에서 SSL 프로토콜은 처음에 네스케이프에서 제안한 프로토콜로써, 브라우저의 폭발적인 확산과 함께 널리 사용되고 있는 보안 프로토콜이다. 현재는 RFC 2246. "The TLS Protocol Version 1.0"으로 표준화되었다. 여기서는 가장 많이 사용되고 있는 두 개의 브라우저(넷스케이프, MSIE)에 사용되고 있는 X.509 규격들을 살펴보도록 한다.

TLS 프로토콜 1.0 및 SSL 프로토콜 3.0은 모두 X.509 v3 인증서를 채택하고 있다. 따라서 이들 SSL/TLS를 사용하는 브라우저들과 호환을 유지하기 위해서는 X.509 v3인증서를 채택해야 한다. 또한, 네스케이프 및 MSIE는 서로 다른 X.509 확장필드를 사용하고 있다. 네스케이프의 경우에는 PKIX에서 권고하고 있는 X.509 확장필드 외에 독자적인 확장필드를 사용하고 있으며, 마이크로소프트의 경우에는 독자적인 확장필드는 없고 PKIX

에서 권고하고 있는 확장필드들 중에 일부를 사용하고 있다. 따라서 SSL/TLS용 인증서의 경우에는 이들 두 브라우저가 지원하는 확장필드들은 기본적으로 지원 가능해야 한다.



(그림 1) Client와 Server를 포함한 시스템 개략도

SSL 프로토콜의 목적과 구조에서 SSL 프로토콜의 주요한 목적은 두 어플리케이션 간의 통신 시 보안과 신뢰성을 제공하는 것이다. 그 프로토콜은 두 레벨로 구성되어 있다. 하위 레벨은 신뢰할 수 있는 전송 프로토콜 위에 위치하며 SSL Record Protocol이라 한다. SSL Record프로토콜은 다양한 상위레벨 프로토콜들을 캡슐화 하는 데에 쓰인다. 캡슐화 된 프로토콜 중의 하나인 SSL Handshake Protocol은 서버와 클라이언트간의 인증을 가능하게 하며, 어플리케이션 프로토콜이 전송되거나 수신되기 전에 이루어지는 암호화 알고리즘, 암호 키에 관한 협상이 가능하게 한다. SSL의 이점중의 하나는 독립적인 어플리케이션 프로토콜이라는 것이다. 상위레벨 프로토콜은 SSL 프로토콜 위에 투명하게 위치 할 수 있다.

3.2 Apache와 ModSSL

mod_ssl에서 사용되는 모든 설정 지시자(configuration directive)와 함께 mod_ssl이 제공하는 user visible feature들에 대하여 설명하며, 이를 통해 mod_ssl의 어떤 특정한 기능이 실제로 어떻게 설정 되는가 혹은 활성화되는가를 설명한다. 각 directive는 Apache 문서에서 표준 Apache directive를 설명하는 방식과 유사한 방식으로 기술되어지는데, 여기에는 directive의 syntax, default, context 등의 요소들이 기술된다.

Mod_ssl에서 사용하는 directive는 크게 세 가지 분류(class)로 나눠진다. 먼저 Global Directive (context가 "server config"인 directive)는 server config 파일에서 <VirtualHost>와 같은 sectioning command 밖에서만 사용될 수 있다. 두 번째는 Per-Server Directive(context가 "server config, virtualhost"인 directive)로서 server config 파일에서 <VirtualHost> 섹션의 밖이나 안에서 모두 사용될 수 있으며, <VirtualHost> 섹션의 밖에서 사용될 때는 메인(Default) 서버에 대한 설정이 된다. 세 번째는 Per-Directory Directive(context가 "server config, virtual host, directory, .htaccess"인 directive)로서 server config 파일과 per-directory .htaccess 파일의 어느 곳에서든 사용될 수 있다. 이 세 가지 class들은 서로의 부분 집합이 되는데, 즉 per-directory의 directive가 per-server와 global context에서 사용될 수 있으며, 또한 per-server class의 directive가 global context에서 사용될 수도 있다.

다른 Apache SSL 솔루션들에 대한 backward compatibility를 위해 mod_ssl이 제공하는 부가적인 directive들과 환경 변수들은 Compatibility Chapter에 기술되어져 있다.

4. 실 험

4.1 SSL에 SEED 적용

인터넷뱅킹에 사용되는 사용자 웹브라우저와

웹서버의 SSL 보안채널에 SEED 알고리즘을 적용하기 위해 아래와 같은 공개S/W와 OS를 사용하여 적용하였다.

한국정보통신기술협회에서 규정한 국가표준 128Bit 블록 암호화 알고리즘 seed[6], SSL이 지원되는 사용자 웹브라우저 mozilla[7], SSL이 지원되는 웹서버 apache[8], apache에 SSL을 사용하기 위한 모듈인 openssl[9], openssl 모듈을 apache에 add-on시켜 apache가 SSL이 지원되도록 하는 모듈인 mod_ssl[10]를 해당 site에서 찾아 사용하였다.

OpenSSL의 SSL에 SEED 적용을 위해 OpenSSL을 컴파일한 후 다음과 같이 OpenSSL을 변경한다.

Mozilla의 SSL에 SEED 적용을 위해 Mozilla를 Compile 한 후 다음과 같이 Mozilla를 변경한다. 먼저 seed 패치가 가해지지 않은 순수한 mozilla.org에서 1.4.1소스를 가져온다. 가져온 소스의 압축을 푼 다음 환경에 따라 행한다.

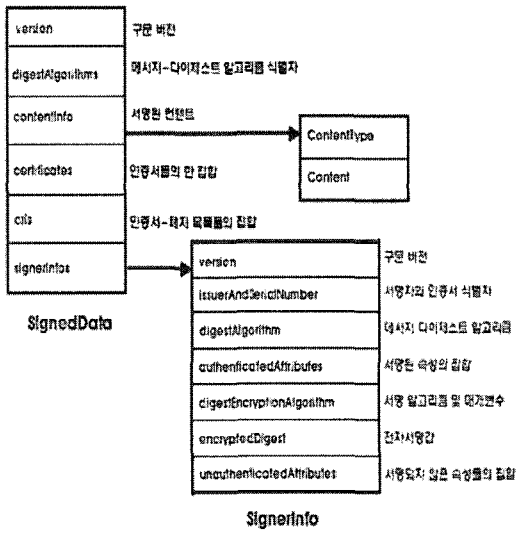
다음 Apache에 SSL 적용 및 설치를 한다. Apache Web Server를 설치하는데 있어서 새로운 기능을 추가하려면 module을 추가해야 한다. SSL을 추가하기 위해서는 mod_ssl을 같이 컴파일 해야 한다. mod_ssl은 SSL 통신을 위한 module로서, 암호화 및 SSL 통신 부분은 openssl을 이용한다. 그러므로, mod_ssl이 compile되기 위해서는 openssl이 함께 compile 되어야 한다. 우선 필요한 S/W들을 다운로드한 다음에 openssl부터 컴파일을 시작한다. 먼저 설치에 필요한 S/W를 다운로드한 후 파일들을 압축 해제한다. 압축을 풀면 각 디렉토리가 생성될 것이다. 다음으로 openssl을 컴파일 한다. 앞 절에서 openssl의 SSL에 SEED적용이 완료가 되었다면 컴파일을 하여 설치한다. openssl을 컴파일하기 앞서 시스템에 대한 환경설정을 해주어야 하는데, configure 명령어는 OS에 맞는 컴파일환경을 제공한다.

4.2 전자서명 SDK 개발

pkcs#7은 전자 서명과 전자 봉투와 같은 암호가 적용된 일반적인 구문을 기술하고 있으며, 이 표준 문서에는 일반적으로 유용한 여섯 개의 항목 타입들로 구성되어 있으며, 각 타입들은 Data Content Type, SignedData Content Type, EnvelopedData Content Type, SigneAndEnvelopedData Content Type, DigestedData Content Type, 그리고 EncrypteData Content Type이다.

본 연구의 범주는 이들 여섯 가지의 타입 중에 SignedData Content Type을 이용한 전자서명 데이터를 생성하는 방식이다.

PKCS#7의 SignedData의 구조는 위와 같으며, SignedData 내용 타입은 그 어떤 타입의 컨텐트와 0 또는 그 이상의 서명자들에 대한 컨텐트의 암호화된 메시지 다이제스트들로 구성된다. 한 서명자에 대한 암호화된 다이제스트는 그 서명자에 대한 컨텐트의 "디지탈 서명(digital signature)"이다.



(그림 2) SignedData 구문 구조

전자서명(PKCS#7)데이터의 생성 시나리오로서 국내에서 사용하는 인터넷 뱅킹을 위한 PKCS#7 데이터는 기본적으로 DER 인코딩을 하여 서버에 보내주게 된다. 전자 서명은 서버에 보내고자 하

는 데이터(송금액 송금인 수금자 등) 개인키를 이용하여서 암호화 하고 그 데이터가 암호화된 시각과 변경 내용 등이 추가되어 하나의 전자서명(PKCS#7) 데이터의 생성 SDK에서 클라이언트 모듈의 설계는 크게 로그인 프로세스와 서명 프로세스로 나누어진다. 로그인 프로세스는 자바 스크립트에서 Login 메소드를 사용하며 진행은 다음과 같이 이루어진다.

- html에서 자바스크립트에 정의되어 있는 함수인 login를 사용한다.
- 이 login는 함수 내부적으로 xpcom 모듈인 pkcs7;1를 오브젝트로 로딩하여 그 오브젝트의 함수인 Login를 부른다.
- 이 함수 Login수는 로그인을 하기 위하여 인증서 선택창을 띄워 사용자의 인증서와 패스워드를 물어 사용자의 인증서를 확인한다.
- 사용자의 인증서가 확인이 되면 그 인증서의 공개키를 PEM 형식의 스트링으로 변환하여 리턴하게 된다.

서명 프로세스는 자바 스크립트에서 SignValue 메소드를 사용하고 순서는 아래와 같다.

- html에서 자바스크립트에 정의되어 있는 함수인 sign를 사용한다.
- 이 sign는 함수 내부적으로 xpcom 모듈인 pkcs7;1를 오브젝트로 로딩하여 그 오브젝트의 함수인 SignValue를 부른다.
- 이 함수 SignValue는 서명을 하기 위하여 인증서 선택창을 띄워 사용자의 인증서와 패스워드를 물어 사용자의 인증서를 확인한다.
- 사용자의 인증서에서 개인키를 읽어 그 개인키를 사용하여 PKCS7 서명 프로세스를 진행하게 된다.
- 서명된 PKCS7 스트링을 결과로 리턴하게 된다. 전자서명(PKCS#12) 데이터 생성 라이브러리전자서명이라는 것이 완료 되는 것이다.

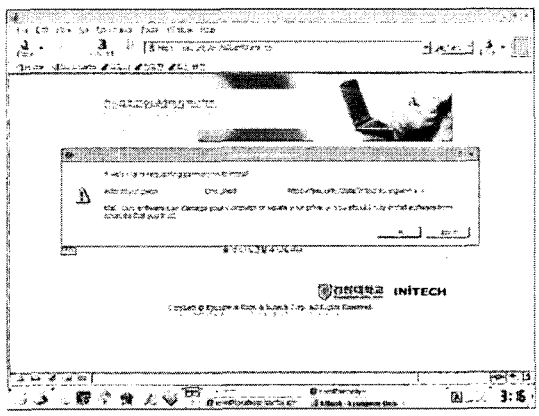
4.3 인터넷 뱅킹 서비스 구현

인터넷 뱅킹 서비스를 구현하는데, Server(Apache SSL) 개발 환경의 Model 및 OS는 COMPAQ evo W8000의 hancom linux 3.1이고, Client(Mozilla) 개발 환경의 Model 및 OS는 redhat Fedora를 활용하였다.

시스템의 설치방법은 다음과 같다.

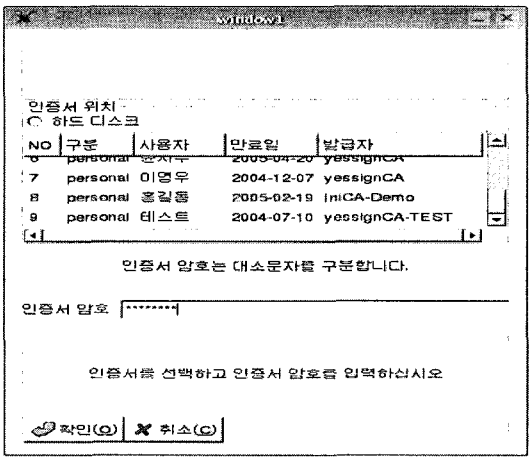
1) Open-SSL 및 Mozilla 소스에 SEED 적용
2) SSL을 이용하는 아파치 서버 기본 구성
   먼저 서버를 구성하기 위한 프로그램을 다운로드 받는다. 다운을 다 받았으면 압축을 해제하고 openssl과 modssl을 기본 설치 방법대로 한다.
3) XPCOM INSTALL에서 non-mozilla-software를 설치
4) SeMoa Verify를 위한 SeMoA Debugging 작업

먼저 첫 페이지가 뜨면 처음 가입 한 사람은 가입 버튼을 눌러 회원 가입 페이지로 이동한다. 이때 회원 가입에 필요한 내용을 입력하면 회원 가입 완료 창이 뜬다. 모든 회원이 인터넷 뱅킹을 사용할 수 있기는 하나 인증서를 선택하는 xpi 클라이언트를 설치해야만 한다. 왼쪽의 인증서클라이언트 설치를 클릭한다. 그러면 인증서 클라이언트 설치 화면이 아래 그림과 같이 나타난다.



(그림 3) 인증서클라이언트 설치 화면의 팝업

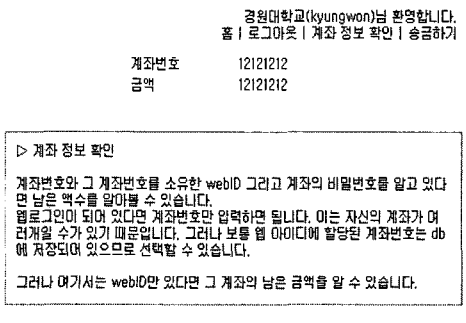
인증서 설치가 완료되면 보통 다른 페이지로 리다이렉트 되나 아직 구현은 되지 않은 상태다. 보통은 mozilla를 껐다 켜야 xpi가 작동하기 때문에 안정적인 테스트를 위해서 껐다 킨 다음 다시 로그인을 하고 인터넷 뱅킹 시작(인증서 로그인)을 클릭하면 페이지 전환이 없이 바로 인증서 선택창이 뜬다.



(그림 4) 인증서 선택창

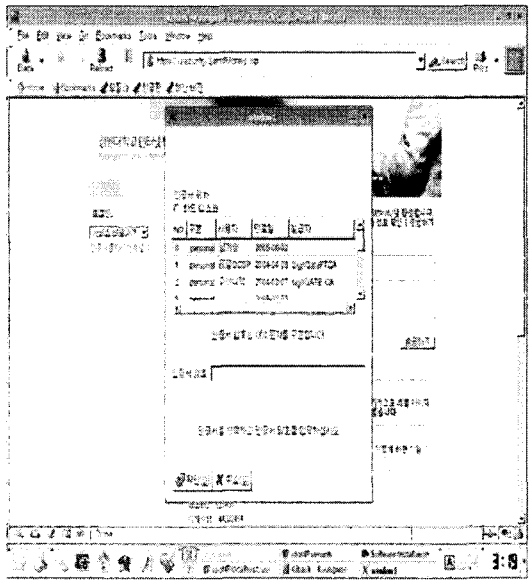
인증서를 골라 인증서의 암호를 넣고 확인 버튼을 누르면 인증서 로그인이 완료된다.

이제 인증서 로그인이 완료 되었고 메인 메뉴에도 계좌 정보 확인 송금하기 기능이 생겼다. 계좌 정보 확인을 누르면 자신의 계좌 번호와 남은 금액을 살펴 볼 수 있다.



(그림 5) 계좌 정보 확인

또한 송금하기를 클릭하면 다시 한 번 인증서선택창이 뜨게 된다.



(그림 6) 송금 시의 재인증

역시 인증서를 선택하고 패스워드를 입력하여 확인을 누르면 송금 완료 페이지를 출력한다.

5. 결 론

이번 연구는 공개소프트에어에서 사용할 PKI 기반 기술을 연구함으로써 리눅스 환경에서도 인터넷 뱅킹 서비스를 제공할 수 있도록 개발하는 것이다. 본 연구 목표에 맞춰 우선 리눅스에서 인터넷 뱅킹서비스를 제공하기 위한 개발이 시행되었는데 구체적인 내용과 절차는 아래와 같이 진행되었다. 먼저 국내 금융서비스(인터넷뱅킹)는 금융감독원의 보안성 심의 기준에 의거하여 반드시 SEED를 이용한 암호화 적용이 이루어져야하기 때문에 사용자 웹 브라우져와 웹 서버의 SSL 보안채널에 SEED 알고리즘을 적용하는 작업을 하

였다. 또한 공개 소프트웨어 환경에서의 전자 지불 시스템을 위한 전자 서명 시스템을 개발하였다. 국내 인터넷뱅킹은 현재 공인인증기관이 발행하는 공인인증서를 통해 인증 및 전자서명 검증이 이루어져야 하는데, 그에 맞춰 공인 인증서 유효성 검증 시스템을 분석 및 개발하였다. 마지막으로 자체 개발한 웹 서버에서는 이미 가상 인터넷 뱅킹 환경이 구축되어 있어 SEED가 포팅 된 모질라 환경을 가지고 있는 클라이언트에서는 인증서를 설치하여 기본 인터넷뱅킹 서비스를 가상으로 받을 수 있으며 인증서 인증 및 전자서명이 정상적으로 작동되고 있다는 것을 확인할 수 있다.

현재 국내 은행에 적용하여 실제로 사용자들에게 제공할 수 있도록 추진 중인데, 시행이 되면 리눅스 사용자들의 인터넷뱅킹 제약을 풀어줄 수 있게 되어 인터넷 뱅킹 사업과 공개소프트웨어 보급에 큰 효과를 기대하고 있다.

향후 연구 분야로써 리눅스 시스템에서 직접 공인인증서를 발급받기 위해서 클라이언트에서 CMP를 구현하여 Mozilla 브라우저에서 Plugin에 포팅하는 연구가 필요하다.

참 고 문 헌

[1] M. Welsh, M. K. Dalheimer, T. Dawson, and L. Kaufman, "RUNNING LINUX", O'REILLY, 2004.

[2] G. Mourani, "Securing & Optimizing LINUX : The Ultimate Solution", Open NA.Com, 2002.

[3] S. McClure, S. Shah, and S. Shah, "Web Hacking : Attacks and Defense", Addison Wesley, 2003.

[4] H. X. Mel, and D. Baker, "Cryptography Decrypted", Addison Wesley, 2001.

[5] A. Carlisle, and L. Steve, "Understanding PKI", Addison Wesley, 2003.

[6] http://sourceforge.net/projects/openseed/

[7] ftp://ftp.mozilla.org/pub/mozilla.org/mozilla/releases/mozilla1.4.1/src/mozilla-1.4.1.tar.gz

[8] http://www.apache.org/dist/httpd/apache_1.3.29.tar.gz

[9] http://www.opens니.org/source/openssl-0.9.4.tar.gz

[10] http://www.mods니.org/source/mod_ssl-2.8.16-1.3.29.tar.gz

[11] http://developer.oss.or.kr

한 명 묵

1980년 연세대학교 공과대학 (공학사)

1987년 뉴욕공과대학교 컴퓨터 공학과(공학석사)

1997년 오사카시립대학교 정보 공학부(공학박사)

1998년~현재 경원대학교 소프트웨어대학 부교수

이 철 수

1975년 육군사관학교 전자계산학과(공학사)

1977년 KAIST 전자계산학과 (공학석사)

1981년 KAIST 전자계산학과 (공학박사)

2003년~현재 경원대학교 소프트웨어대학 교수