Proceedings of KFIS Spring Conference 2004 Volume 14, Number 1

공개 소프트웨어 환경에서의 인터넷 뱅킹 서비스를 위한 PKI 기반기술

PKI based Technology for Internet Banking Service in Open Software Environment

김금실**, 김균섭**, 한명묵*
경원대학교 일반대학원 전자계산학과
Jin-Shi Jin**, Kyun-Soup Kim**, Myung-Mook Han*
Graduate of Computer Science, Kyungwon Univ.
E-mail: hakuna1103@hotmail.com

요 약

인터넷을 기반으로 하는 금융서비스를 제공함에 있어 보안성에 대한 필요성이 최근 들어 매우 중요시되어져가고 있으며, 이 분야에 대한 많은 연구가 진행 되어 오고 있다. 국내 대부분의 은행 기관에서는 인터넷 뱅킹 서비스를 지원하고 있으나, 그 서비스 이용에 있어 윈도우 사용자에 국한되어 있는 실정이다. 본 논문에서는 리눅스 기반에서 보다 더 안전한 인터넷 뱅킹 서비스를 지원하기 위한 PKI 기반 기술을 제안한다.

키워드: 인터넷 뱅킹, PKI, LINUX, SSL/TLS, 전자서명, Crypto Library

1. 서론

최근 전자상거래의 활성화로 인터넷과 같은 개방형 네트워크 상에서 다양한 금융 서비스 제공의 필요성이 증대되고 있다. 전자자금이체 서비스, 신용카드를 매체로 하는 전자 지불 시스템 및 전자화폐 등과 같은 다양한 전자금융 서비스들이 개방형 네트워크 상에서 안전하게 처리되기 위해서는 거래에 대한 기밀성, 통신 상대방의 인증, 무결성 확보 및 익명성 제공 등과 같은 보안 서비스 이용이 필수적이다.

인터넷뱅킹은 인터넷이 연결된 PC 또는 인터넷이 지원되는 휴대폰·TV 등을 이용해 고객이 직접 금융정보를 조회하거나 송금(이체), 대출 및 상환, 해외송금 등의 서비스를 이용할 수 있도록 개발된 첨단 금융서비스다. 인터넷뱅킹은 인터넷이 연결된 단말 기가 있는 곳이면 어디든지 시간과 장소에 구애받지 않고 바로 은행계좌에 접속할 수 있는 것이 장점이다.

인터넷뱅킹을 통한 각종 조회나 자금이체 및 대출서비스는 2001년부터 지속적인 상승세를 보이고 있는데, 이러한 인터넷뱅킹 이용고객의 증가에 따라 여러 가지 보안 문제들도 대두 되고 있다.인터넷 뱅킹은 우리에게 은행 창구를 방문하는 번거로움을 줄여주는 획기적인 IT 산업의 결과물이지만, 그와 더불어 국내에서는 MS의 Windows와 인터넷 익스플로러 궁합이 아니면 쓰지 못하는 IT 산업의 절름발이 결과물이다.

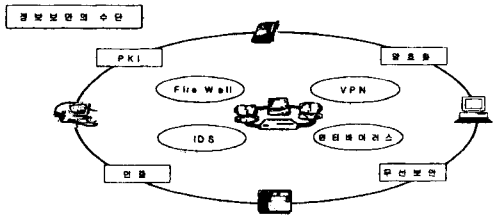
본 논문에서는 공개소프트웨어 환경에서의 인터넷뱅킹을 위한 보안문제를 다루고자 한다. 2장에서는 인터넷 뱅킹 보안과 관련된 기반기술을 기술하고 3장에서는 본 논문에서 제안한 리눅스 환경에서의 인터넷뱅킹을 위한 보안 기술을 설명하고 4장에서는 구현의 과정에 대해 간략히 기술한다. 마지막으로 5장에서 결론 및 향후 추가개발 할 계획으로 끝을 맺는다.

2. 인터넷 뱅킹을 위한 기반 보안기술

2.1 전자상거래 보안

상거래에서 가장 기본적으로 요구되는 사항은 신뢰성이다. 그러나 전통적인 상거래에서의 대면거래와 달리 전자 상거래에서 당사자들은 개방된 네트워크 전자 환경에서 상거래 활동이 이루어지는 것이므로 우선적으로 당사자간의 신뢰를 형성하는 것이 최우선이다. 즉, 정보시스템과 기술적이 메커니즘에 대한 신뢰성, 네트워크 상에서 제공되는 서비스의 안전성, 그리고 전자상거래 관련법, 제도에 대한 신뢰성이 필요하다.

정보보안은 시스템에의 접근을 차단하는 방법이 아니라 개방형 시스템과 같이 타인에 의한 침해의 위험성이 상존해 있는 환경에서 컴퓨터에 의하여 생성된 정보 자체 또는 정보의 흐름을 보호함으로써 권한 없는 자에 의한 정보의 훼손을 방지하는 보안 방법을 말한다[1].



<그림 1> 정보보안의 수단

2.2 Seed알고리즘

Seed는 민간부문에서의 정보와 개인 프라이버시 등을 보호하기 위하여 한국정보보호진흥원(구,한국정보보호센터)과 ETRI주도하에 개발된 대칭키 방식의 128비트 블럭암호 알고리즘으로 1999년 9월 국내 단체표준화 (TTA.KO-12.0004)를 완료하였다[1].

2.3 PKI(Public Key Infrastructure) 기술

PKI는 공개키와 개인키 간의 합치성(Correspondence)의 특성을 이용하여 전자문서를 수신한 상대방이 송신자의 신원확인, 전자문서의 위/변조 방지, 전자문서의 송신사실의 부인 방지를 할 수 있는 기술을 말한다.

즉, 개인키(Private Key)와 공개키(Public Key)라는 두 개의 키를 이용하여 문서를 전자서명하고 이를 검증하는 기술로, 개인키는 사용자 자신만이 알고 있는 키를 말하며 사용자는 이 키를 이용하여 문서에 전자서명을 하게 된다. 공개키는 이 키에 대응하는 키로서, 문서를 수신할 상대방은 공개키를 이용하여 전자서명된 문서를 검증한다. 개인키로 전자서명 된 문서는 이에 대응하는 공개키를 가진 사람만이 그 서명을 검증할 수 있다.

2.4 SSL(Secure Socket Layer) /TLS(Transport Layer Security)

SSL은 인터넷을 통해 전달되는 정보의 안전한 거래를 허용하기 위해 Netscape사에서 개발한 인터넷 통신 규약 프로토콜이다. SSL은 데이터의 암호화, 서버의 인증, 메시지의 무결성을 제공한다. 안전한 전자 거래를 위한 프로토콜을 설계함에 있어서 공개키 암호 기술이 필요하게 되었고, 신뢰기관의 공개키 무결성 보장을 위해서 인증서의 필요성이 대두되었다. 이에 인증서 발급을 위한 인증기관(CA)이 구축이 되고, 인증기관들 간의 유기적 결합관계가 성립되면서 공개키 기반구조를 이룬다[2].

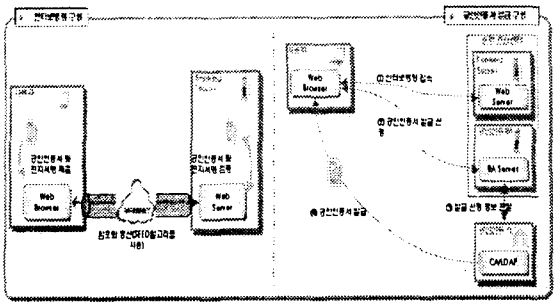
TLS 프로토콜 1.0 및 SSL 프로토콜 3.0은 모두 X.509 v3 인증서를 채택하고 있다. 따라서 이들 SSL/TLS를 사용하는 브라우저들과 호환을 유지하기 위해서는 X.509 v3인증서를 채택해야 한다. 또한, 네스케이프 및 MSIE는 서로 다른 X.509 확장필드를 사용하고 있다. 따라서 SSL/TLS용 인증서의 경우에는 이들 두 브라우저가 지원하는 확장필드들은 기본적으로 지원 가능해야 한다[3].

현재 세계적으로 많은 PKI구축이 이루어져 있다. 응용기술들로 PEM, S/MIME, SET, SSL 등이 있고, 사용 인터페이스로는 GSS-API, Crypto API, CDSA, PKCS#11등이 있다. PKCS#11(Cryptographic Token Interface Standard)은 일반적으로 CAPI라고 불리는 보안 서비스 API를 정의한다.

3.공개소프트웨어 환경에서 PKI기반 인터넷뱅킹 보안 기술

3.1 인터넷뱅킹의 구성

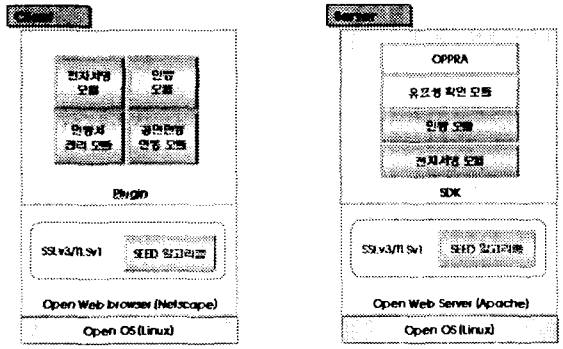
인터넷 뱅킹의 구성을 살펴보면 그림 2에서 표시한 것처럼 사용자는 인터넷 뱅킹 웹서버에 접속하여 서비스를 요청하면 공인인증기관에서 일정한 절차를 거쳐 공인인증서를 발급받는다. 그리고 공인인증서와 전자서명을 제출하여 암호화 통신을 거쳐 웹 서버에서 공인인증서 및 전자서명을 검증받아 원하는 뱅킹서비스를 받을 수 있다.



<그림 2> 인터넷 뱅킹의 구성

3.2 서버와 클라이언트 구조

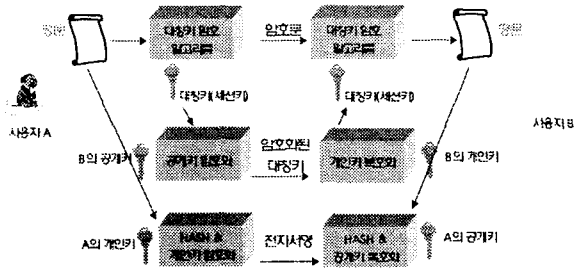
본 논문에서 제안한 시스템의 서버/클라이언트 구조는 그림에서 보시다 시피 공개소프트웨어 환경에서 인터넷 뱅킹 시스템의 웹 서버는 CPPRA,유효성 확인 모듈, 인증 모듈, 전자서명 모듈로 구성되며 클라이언트는 전자서명 모듈, 인증모듈, 인증서 관리 모듈, 공인인증 연동 모듈로 구성된다. 여기서 본 논문에서 개발할 모듈은: 1)금융서비스를 위한 데이터 암호 알고리즘으로 seed 국가표준을 사용하여야 하므로 공개소프트웨어 웹 브라우저와 웹서버에 Seed 암호 알고리즘이 지원되어야 한다.2)웹브라우저에는 응용서비스 데이터에 대한 전자서명 기능이 제공되지 않으므로 금융거래를 위한 데이터 전자서명을 할 수 있도록 하기 위한 Plug-in 모듈을 개발한다.3)국내 6개 공인인증 기관들이 발급하는 공인인증서에 대한 발급/폐기/갱신 기능과 인증서 복사/삭제/형식변환 등의 관리 기능을 제공하는 모듈을 개발한다.4)웹 브라우저가 서버에 전달하는 전자서명 정보에 대한 검증 역할을 수행하는 서버 모듈이 필요하다.5)인터넷뱅킹 환경을 제공하기 위한 사용자 UI가 KISA에서 지정한 표준 규격으로 나와 있으므로 이를 구현한다.



<그림 3> Client와 Server의 개략도

3.3 제안한 암호 알고리즘

본 논문에서 제안한 암호화 방법은 기존에 공개키 암호화 방법의 취약점을 보완하고 또한 리눅스 환경에 적용하기 위해 일차적으로 평문을 seed 알고리즘으로 대칭키 암호화 방법을 이용하여 암호하고 거기서 사용되는 대칭키를 공개키 암호화 방법으로 암호화하여 교환하는 방법을 제안하였다. 알고리즘 구조는 그림 4와 같다.



<그림 4> 제안한 암호화 알고리즘

4. 구현 및 성능평가

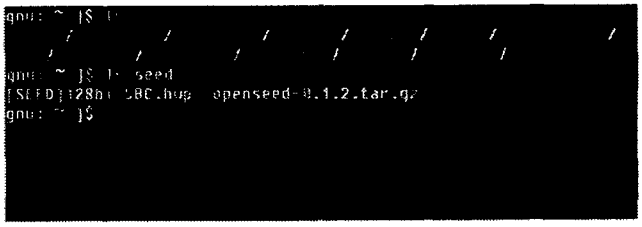
4.1 암호화부문-SSL 적용

개발환경이 구축되면 우선 Seed알고리즘을 Open Source에 포팅하는 작업을 진행한다. 본 논문에서는 mozilla 1.5버전과 apache1.3버전을 사용했다.

작업의 일부과정을 설명하자면 아래와 같다.

1) openseed 소스를 '/crypto'디렉토리 밑에 Seed란 디렉토리를 생성한 후 복사한다[4].
2) './crypto/objects/objects.h'에 Seed관련 정의를 추가한 다음 Seed 알고리즘 관련 파일을 './crypto/evp/e_cbc_d.c'파일로 복사하고, './crypto/evp/evp.7h' 파일안에 seed.h 헤더파일을 추가한다.
3) './cryto/evp/evp.h' 파일 안에 있는 EVP.CIPHER_CTX 구조체 안에 있는 C 구조 체 안에 'seed.h' 파일 안에서 정의 된 SEED_KEY_SCHEDULE 변수 seed_ks를 선언한다.
4) init_key 함수와 cipher 함수 이름을 seed에 맞게 개명하고 배열과 배열 값 함수 포인터를 seed에 맞게 수정한다. 키 사이를 seed키 사이즈로 수정한다.
5) cbc_cipher 함수 내부에서 ctx->encrypt 의 값에 따라 encrypt 와 decrypt를 분기 한다.

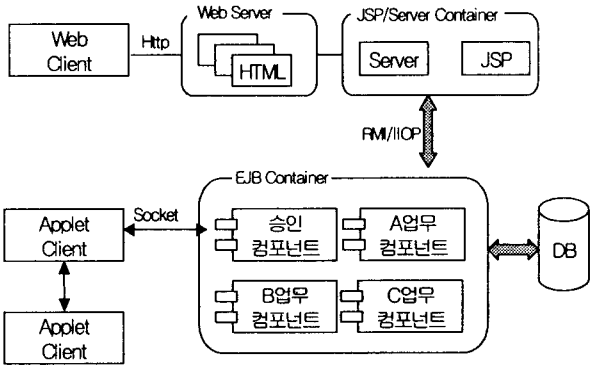
그림 5는 seed 디렉토리를 생성하여 seed 소스를 추가한 초기 모습이다.



<그림 5> seed 디렉토리 생성모습

4.2 서버/클라이언트 구축

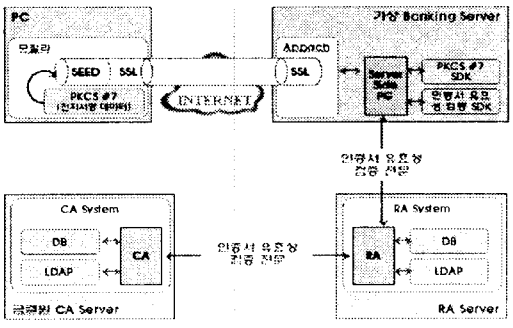
현재 뱅킹 컴포넌트 시스템의 구성 및 기능은 그림 6의 구조도에서 보는 바와 같이 jsp/서블릿/애플릿 위주의 클라이언트 측과 업무컴포넌트 위주의 서버 측으로 나눌 수 있다. 텔러는 웹 브라우저에서 JSP를 통해 서비스를 요청하고 이 요청은 해당 업무컴포넌트에 전달되어 트랜잭션의 유효성 검사, 승인처리를 거친 후 다른 업무컴포넌트들의 협조를 받아 처리된다. 모든 처리가 끝나면 해당 업무컴포넌트는 클라이언트 측에 처리결과를 반환한다[5].



<그림 6> 서버 클라이언트 구조

개발환경으로는 JDK1.3과 Tomcat을 설치하고 PKCS#7 데이터와 금결원 OPPRA스펙을 분석한다. 그리고 윈도우상에서 클라이언트환경을 구축하고 SEVER도 구축해야하는데 서버구축에는 또한 다음과 같은 세 가지가 포함된다. 즉, PKSC#7 Opensource를 수집하여 설치, 공인인증서 유효성 검증과 SDK 구현 및 공인인증서 전자 서명 Server Page 개발 등이 있다.

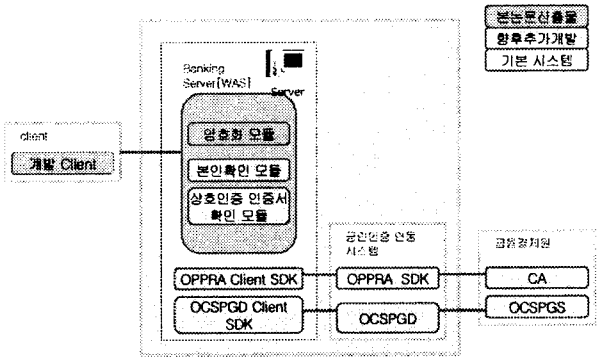
앞의 두 부분이 구현이 완성되면 그림 7에서처럼 통합테스트를 통하여 시스템의 가동성을 테스트할 예정이다.



<그림 7> 프로젝트 인증서 유효성 검증

5. 결론 및 향후발전 방향

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.



<그림 8>향후 추가 개발 부분

이에, 본 논문에서는 리눅스상에서 보다 안전한 인터넷뱅킹을 위한 보안기술을 제안하였으며 이를 통해 증가되고 있는 리눅스 환경 사용자들도 더욱 편리하고 신뢰성 있는 금융서비스를 이용할 수 있게 한다. 하지만 그 어떤 보안도 반드시 취약점이 있는 만큼 지금 개발한 기초에서 더욱더 경고한 시스템을 위하여 그림 8과 같은 부분에서 더 추가연구를 할 계획이다.

참고문헌

[1] 이경삼,"전자상거래를 위한 SSL기반의 전자지불시스템 설계" 호남대학교. 석사학위논문, pp.12-47, 2002

[2] 윤한성,"인터넷뱅킹을 통한 전자지불체계 모델" 産業經濟,Vol.12, 2001.

[3] 신원,이경현,"안전한 인트라넷을 위한 보안모델"멀티미디어학회 논문집 Vol.2, No.2, 1999.

[4] P.Paillier, "Pubic-Key Cryptosystem Based on Composite Degree Residuosity Classes" *Advanced in Cryptology-Eurocryp' 99,* Springer-Velag, Lecture Notes in Computer Science. Springer-Verlag. pp.223-238, 1999.

[5] 안태광,김병기 "웹기반 뱅킹컴포넌트 시스템에서 승인시스템의 설계 및 구현" 정보처리학회 논문집 제8-D, No.6, 2001.

[6] 강영구,"전자상거래 보안에 기반 한 암호 시스템의 설계" 서울산업대학교, 석사학위논문, pp.8-37, 2000.