스마트폰 환경에서 USIM 정보를 이용한 효율적인 전자서명 기법

조강희, 전문석
숭실대학교 일반대학원 컴퓨터학과
e-mail : chokang82, mjun@ssu.ac.kr

An Efficient Electronic Signature using USIM Information on Smart phone

Kang-Hee Cho, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

아이폰 출시 이후로 스마트폰의 강세를 이루는 현재, 스마트폰의 보안문제도 많은 화제가 되고 있다. 그 중에서도 Active X를 설치해야 사용할 수 있는 공인인증서가 스마트폰 환경에서 사용할 수 없는 문제가 제기 되었다. 그 대안으로 KISA나 ETRI에서 스마트폰에서 공인인증서를 사용할 수 있는 앱(Application)을 개발 중이지만 공인인증서를 사용하지 않고 USIM정보와 해시함수를 이용하여 기존의 PKI시스템보다 시스템 복잡도를 낮추며 공개키 프레임워크의 확립 및 관리와 관련된 비용절감 효과를 볼 수 있는 시스템을 제안한다.

1. 서론

애플사에서 아이폰 출시 이후 스마트폰에 대한 관심도가 높아져 우리나라도 스마트폰 개발에 힘쓰고 있다. 스마트폰이란 휴대폰에 컴퓨터 기능을 추가한 지능형 휴대폰으로 휴대폰 기능에 충실하면서도 PDA나 인터넷 기능 등이 일부 추가되며, 수기 방식의 입력장치와 터치스크린 등 보다 사용에 편리한 인터페이스를 갖춘 기기이다. 통신사의 3G망이나 Wi-Fi망을 통해 인터넷에 접속하여 이메일, 웹브라우징, 게임 등 단말기로서의 기능도 수행한다.

현재 스마트폰에서 은행사이트 로그인은 원활하지 못한 상태이다. 기존의 PC에서 은행사이트 접속 시 전자금융거래법 시행세칙 29조에서 요구 사항 중인 키보드보안, 안티바이러스 및 개인 방화벽 소프트웨어를 설치해야 하는데 이 기능들을 위해서 바이러니 플러그인이 사용되고 있다.[1] 하지만 스마트폰에서의 모바일 웹은 바이러니 플러그인 설치가 불가능하여 은행용 앱이 따로 출시되어 다운로드 한 뒤 인터넷 뱅킹을 이용할 수 있다. 이러한 문제들로 인해 정부는 전자금융거래시 공인인증서 의무사용 규정을 없애고 금융기관이 직접 인증방법을 선택할 수 있도록 하는 방안을 확정했다. 방송통신위원회는 '전자금융거래 인증방법의 안전성 가이드라인'을 발표했다. 가이드라인에는 전자금융거래시 적용될 인증방법이 갖추어야 할 기술적 안전성 요건을 규정한 것으로, 이용자 인증, 서버 인증, 통신채널 암호화, 거래내역의 무결성, 거래내역의 부인방지 기능 등 5개 항목이 제시되었다.[2]

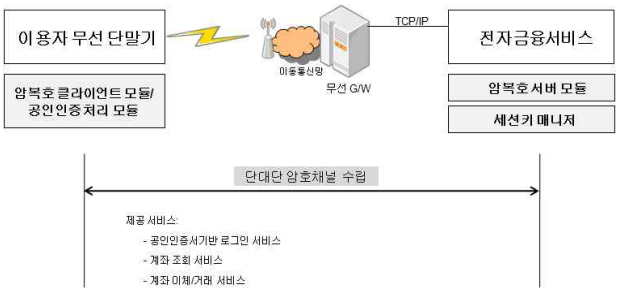
본 논문에서는 스마트폰 사용자들의 편의성을 고려해 사용자 인증서를 사용하지 않고 USIM정보를 이용하여 사용자를 인증한다. 또한 스마트폰의 오버헤드를 감안하여 공인인증서 전자서명을 대체할 효율적인 프로토콜을 제안 한다.

2. 관련연구

2.1. 모바일 폰뱅킹

모바일 폰뱅킹은 사용자가 소유한 휴대폰을 활용하여 조회, 거래 등 전자 금융거래를 이용할 수 있는 서비스이다. 최근 제공되고 있는 일부 폰뱅킹 서비스에서는 공인인증서기반의 로그인, 로그인 후 예금조회, 계좌 이체 등의 서비스를 제공하고 이는 기존 PC에서 발급받은 인증서를 스마트폰으로 이동하여

사용할 수 있도록 인증서 이동 서비스도 제공하고 있다. [그림 1]은 모바일 폰뱅킹 서비스의 흐름을 보여주고 있다.[3]

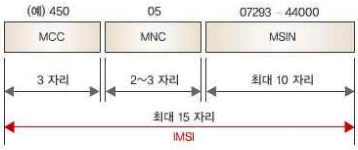


[그림 1] 모바일 폰뱅킹 서비스 흐름도

모바일 폰뱅킹에서 제공하는 서비스는 각 이동통신사별 서비스 접속 방법에 따라 모바일 폰뱅킹 프로그림 기동 후 인증서 기반의 로그인을 수행하고 이용자가 보유한 전자금융상품에 대한 조회와 인증서 발급, 타행 등록, 인증서 갱신, 폐기 등 공인인증서 관리 서비스가 있다. 서비스 형태에 따른 암호기법으로 인증에는 1024비트의 RSA, SHA1withRSA를 사용하고 조회는 128비트의 SEED와 160비트의 HMACSHA1을 사용한다. 거래에는 1024비트의 SHA1withRSA 암호 알고리즘을 사용한다.

2.2. USIM

USIM은 WCDMA 네트워크 접속 및 가입자 인증 소프트웨어 모듈로 3G모바일 단말에 꽂히는 통신용 스마트 카드인 UICC에 탑재되어 구동된다.[4] USIM 은 GSM의 SIM과 동일하게 사용자 프로파일, UMTS(Universal Mobile Telecommunication System)상에서의 인증을 위한 키, 사용자 데이터등을 저장하고 있으며, SIM과 같이 단말기에 삽입과 제거가 가능한 장치이다. USIM의 기술 개발은 인증 프로세스의 유연성과 보다 강력한 보안에 초점을 맞추기 위해 공개키 기반구조의 사용을 목표로 진행되었으나, 짧은 연구기간과 공개키 기반 구조를 적용하는데 있어서의 복잡성으로 인해 대칭키 시스템을 사용하고 있다. USIM의 보안특성으로 사용자 신원의 기밀성, 객체인증, 기밀성, 데이터 무결성 등이 있다.[5] USIM에는 IMSI(International Mobile Subscriber Identity)라는 정보가 있는데 이는 GSM 이동통신망에서 개별 통신가입자에게 할당되는 국제적으로 유일한 식별번호 이다. IMSI 구조는 다음 [그림2]와 같다. MCC와 MNC는 이동전화 가입자의 Home network를 전 세계 어떠한 망에서도 유일하게 식별한다. 즉, IMSI는 Visited network(로밍 서비스를 제공하는 타 network)가 최대 처음 6digit를 분석해서 Home network를 조회할 수 있는 구조로 되어 있다. MSIN은 MCC와 MNC가 주어진 경우 이동전화 단말기를 유일하게 식별 한다.



약어	명칭	할당 주체
MCC	Mobile Country Code	ITU(TSB)
MNC	Mobile Network Code	National Authority또는 TSB
MSIN	Mobile Subscriber Identification Number	National Authority(국내) (MNC를 할당 받은 사업자)

[그림 2] IMSI 구조

2.3. HMAC

HMAC은 Bellare, Canetti, Krawczyk에 의해 제안된 해시함수 기반 메시지 인증 코드로[6] 송,수신자끼리 비밀키를 공유하여 비밀키를 모르면 해시 결과값을 만들 수 없어 사전에 비밀키를 공유한 사용자들만 인증할 수 있는 기술이다. m은 메시지, K는 비밀키, opad와 ipad는 고정된 1블록 크기의 상수값 일 때, HMAC은 다음과 같이 정의된다.

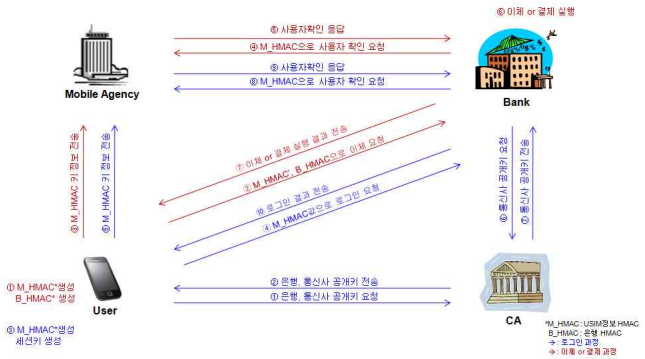
$$HMAC(K, m) = H((K \oplus opad) \parallel H((K \oplus ipad) \parallel m))$$

HMAC은 단순한 구조로 SSL, TLS, SSH, IPsec등 다양한 프로토콜 환경에서 이용되고 안전성 증명이 이루어져 있다.

3. 제안 시스템

본 논문에서 제안하는 내용은 현재 공인인증서로 시행되고 있는 사용자 인증을 사용자의 USIM을 사용하여 통신사가 사용자를 보증하는 시스템이다. 이 과정에서 USIM정보의 노출을 최소화하기 위해 HMAC을 사용하게 되는데 여기서 사용되는 키 값은 해당 사이트의 ID와 패스워드, 사용자가 임의로 생성한 값을 연접하여 키로 사용한다. 다음 [그림2]에는 제안시스템의 구성도이다. 제안 사항은 크게 로그인단계와 계좌이체 단계로 나누어진다. 계좌 조회 단계는 로그인 과정에서 보안핸드쉐이킹으로 생성된 세션키로 암,복호화 하여 서비스를 받는다. 이

는 기존의 공인인증서 계좌조회 시스템과 같기 때문에 생략하기로 한다.



[그림 2] 제안 시스템 구성도

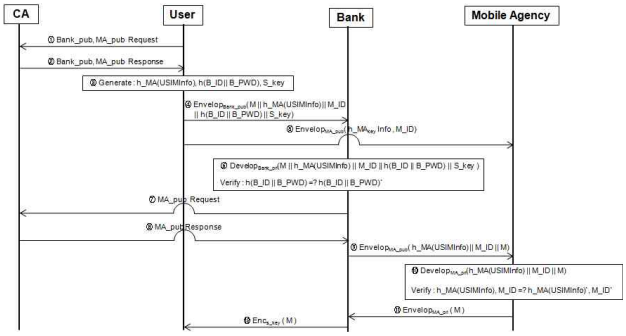
본 논문의 가정 사항으로 사용자는 해당 사이트에 이미 가입된 상태이고 스마트폰 단말에 금융기관 서버와 종단 간 보안 세션을 수립하고 송,수신 메시지에 대한 암,복호화 처리 기능을 제공하는 모듈이 설치되어 있어야 한다. 금융기관과 통신사에도 스마트폰에 설치된 암,복호화 처리 모듈과 종단 간 보안 세션을 수립하고 송,수신 메시지에 대한 암,복호화 처리 기능을 제공하는 모듈이 설치되어야 한다. 그리고 금융기관엔 통신사가 사용자를 보증할 때 쓰일 서명 검증 모듈이 설치되어 있어야 한다.

다음은 상세 프로토콜에 쓰이는 약어를 정리한 것이다.

- Bank_pub : 은행 공개키
- Bank_pri : 은행 개인키
- MA_pub : 통신사 공개키
- MA_pri : 통신사 개인키
- h_MA: 통신사 HMAC
- h_MA_{key} Info : HMAC 키정보
- USIMInfo: USIM 정보
- M : 메시지
- M_ID : 통신사용 ID
- B_ID : 은행용 ID
- B_PWD : 은행용 패스워드
- S_key : 세션키
- h_Bank: 은행 HMAC
- h_Bank_{key} Info : HMAC 키정보
- TS : 타임스탬프
- S_key : 세션키

3.1. 로그인 프로토콜

로그인 단계는 공인인증서기반 로그인을 대체 할 USIM정보를 HMAC하여 로그인을 수행한다. 로그인 단계는 ID, 패스워드 방식도 있지만 공인인증서 로그인 시스템을 대체할 만한 프로토콜을 제안 한다. 상세 프로토콜 내용은 다음 [그림3]과 같다.



[그림 3] 로그인 프로토콜

[1단계] 사용자는 CA에게 은행과 통신사의 공개키를 요청한다.

[2단계] CA는 사용자에게 은행과 통신사의 공개키를 전송한다.

[3단계] USIM정보를 통신사 사이트에 가입한 ID, 비밀번호, 사용자가 임의로 생성한 값을 키로 HMAC을 생성하고 은행에 로그인하기 위해 은행사이트에 가입한 ID와 비밀번호를 해시한 값, 은행과 통신하기 위한 세션키를 생성한다.

[4단계] 로그인 메시지와 통신사용 HMAC값, 통신사용 ID, 은행 로그인용 해시, 세션키를 은행의 공개키로 암호화 하여 은행에 전송한다.

[5단계] USIM정보를 HMAC하기 위해 사용한 임의의 값과 통신사용 ID를 통신사의 공개키로 암호화 하여 통신사에 전송한다.

[6단계] 은행은 수신한 암호문을 복호화 한 후 사용자의 ID와 패스워드를 해시하여 사용자에게 받은 해시값과 비교하여 사용자를 1차 검증한다.

[7단계] 은행은 CA에게 통신사의 공개키를 요청한다.

[8단계] CA는 은행에게 통신사의 공개키를 전송한다.

[9단계] 사용자에게 받은 HMAC값과 사용자의 통신사용 ID를 통신사의 공개키로 암호화 후 통신사에게 사용자 인증을 요청한다.

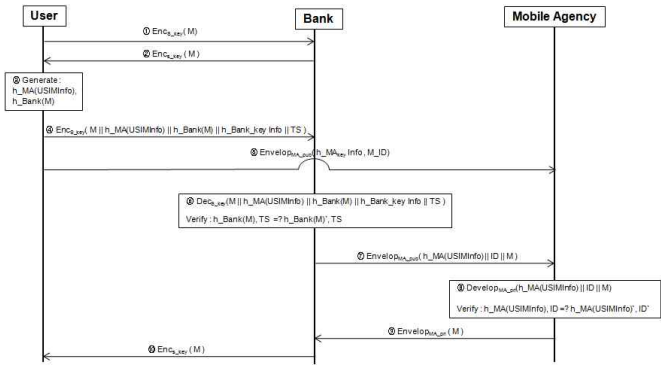
[10단계] 통신사는 은행에게 받은 암호문을 복호화 한 후 사용자에게 받았던 HMAC 키 정보를 토대로 사용자 USIM정보를 HMAC하여 은행에 받은 사용자 HMAC값과 비교하여 사용자를 검증한다.

[11단계] 검증결과를 통신사의 개인키로 서명하여 은행에 전송한다.

[12단계] 은행은 통신사에게 받은 결과로 사용자의 로그인 결과를 사용자에게 받은 세션키로 암호화 후 사용자에게 전송한다.

3.2. 계좌이체 프로토콜

계좌이체 프로토콜은 전자서명을 대체하기 위해 사용자는 로그인단계와 다른 USIM정보 HMAC값을 생성해야 한다. 여기서 은행용 HMAC을 생성하는 이유는 통신사의 내부 공격을 보호하기 위해 은행의 ID와 패스워드, 사용자가 임의로 생성한 값을 키로 하여 HMAC을 사용한다. 상세프로토콜은 다음 [그림 4]와 같다.



[그림 4] 계좌이체 프로토콜

[1단계] 사용자는 계좌이체를 하기위해 은행에 이체요청 전문 세션키로 암호화 하여 전송한다.

[2단계] 은행은 사용자에게 이체 가능한 결과를 세션키로 암호화 하여 전송한다.

[3단계] 사용자는 이체를 실행하기 위해 사용자의 USIM정보를 HMAC하고 이체실행 메시지를 은행사이트용 ID와 패스워드, 사용자 임의의 값으로 HMAC을 생성한다.

[4단계] 사용자는 계좌이체 실행 메시지와 방금 생성한 HMAC값들, 은행용 HMAC을 생성하기 위해 입력했던 임의의 값과 타임스탬프를 세션키로 암호화 하여 은행에 전송한다.

[5단계] 계좌이체를 하기위해 USIM정보를 HMAC할 때 생성했던 임의의 값과 통신사용 ID를 통신사의 공개키로 암호화 하여 통신사에 전송한다.

[6단계] 은행은 사용자에게 받은 암호문을 복호화한 후 계좌이체 메시지를 HMAC하고 사용자에게 받은 은행용 HMAC값과 타임스탬프를 비교하여 사용자를 1차 검증한다.

[7단계] 사용자에게 받은 USIM HMAC값과 통신사용 ID를 통신사 공개키로 암호화하여 통신사에게 사용자 인증을 요청한다.

[8단계] 통신사는 은행에게 받은 암호문을 복호화한 후 사용자에게 받은 HMAC키 정보로 통신사가 알고 있는 사용자 USIM정보를 HMAC하여 은행에게 받은 사용자의 HMAC값과 비교하여 사용자를 검증한다.

[9단계] 통신사의 개인키로 사용자 검증 결과를 서명하여 은행에 전송한다.

[10단계] 통신사에게 받은 검증결과를 토대로 이체를 수행한 후 이체 결과를 세션키로 암호화 하여 사용자에게 전송한다.

4. 결론

본 논문은 공인인증서를 대체할 수단으로 사용자의 USIM정보를 이용하여 통신사가 사용자를 보증한다. 그렇게 함으로써 사용자의 인증서가 필요 없어지고 수많은 사용자들의 인증서 관리가 필요 없어져 인증서 관리비용을 절감할 수 있다. 또한 현재 시행중인 공인인증서의 전자서명법은 메시지를 해시하여 사용자의 개인키로 전자서명 후 다시 은행용 공개키로 암호화하여 전송하는 signedEnvelop 방식을 사용하여 두 번의 암호화 과정을 거치게 된다. 하지만 본 논문에서 제안하는 내용은 HMAC을 사용하여 한 번의 암호화 과정만을 사용함으로써 경량화된 프로토콜을 제안한다.

참고문헌

[1] 이동산, “스마트폰과 전자상거래”, TTA Journal No.128

[2] 국무총리실, “전자금융거래 인증방법의 안전성 가이드라인”, 보도자료 2010.5.31

[3] 금융보안연구원, “금융부문 암호기술 관리 가이드”, 금보원 2010-001

[4] http://ko.wikipedia.org/wiki/USIM

[5] 원동규 외 4, “SIM/USIM의 표준화 동향에 관한 연구” 정보보호학회지 제 15권 제 3호, 2005.6

[6] M.Bellare, R.Canetti, and H.Krawczyk, "Keying Hash Functions for Message Authentication" Advances in Cryptology - CRYPTO 1996, LNCS 1109, pp. 1-15. 4996