스마트폰 공인인증서의 안전성 향상을 위한 기법

김대중, 장윤석
대진대학교 컴퓨터공학과
e-mail:djnara@gmail.com

An Enhanced PKI Security Management on Smartphone

Dae-jung Kim, Yun Seok Chang
Dept of Computer Engineering, Daejin University

요 약

공인인증서를 사용하는 스마트폰 응용에서는 공인인증서를 스마트폰의 내부 메모리에 내장하거나 SD 메모리에 저장하여 스마트폰에 설치된 응용 프로그램이 이를 접근하는 방법을 사용한다. 그러나 공인인증서를 스마트폰의 메모리에 저장하여 사용하는 경우, 공인인증서의 암호만 알면 타인의 공인인증서를 임의의 스마트폰에 설치하여 사용할 수 있다는 문제점을 안고 있다. 이와 같은 문제점을 해결하고 메모리에 저장되는 공인인증서의 보안성을 높이기 위하여 본 논문에서는 스마트폰의 IMEI와 USIM의 IMSI를 키로 사용하여 스마트폰과 사용자를 식별함으로써 특정한 개인의 스마트폰에서만 해당 개인의 공인인증서를 사용할 수 있도록 하는 방법을 제안하고, 그 효율성을 분석하였다.

1. 서론

PDA, 휴대전화, 디지털카메라, 네비게이션, 스마트폰과 같은 임베디드 디바이스의 발달은 일상생활에서 사용자들에게 편리함을 가져다주었다. 그 중에서도 최근 가장 이슈가 되는 임베디드 디바이스는 스마트폰으로, 전화기능과 더불어 전자우편, 인터넷, 게임, 문서관리, 금융거래 등 PC와 같은 고급기능들을 제공한다. 즉, 스마트폰은 전화 기능이 있는 소형 컴퓨터라고 할 수 있다.

스마트폰이 제공하는 수많은 기능 중에서도 커다란 이슈로 주목받는 부분은 인터넷 뱅킹이나 쇼핑몰 결제등과 같은 개인 금융 서비스 분야이다. 이는 모바일 환경에서의 작은 보안상의 위험이라도 큰 금전적인 피해를 유발할 수 있는 가능성이 존재할 수 있기 때문이다.[7]

이러한 피해를 줄이기 위하여 금융, 쇼핑 분야에서도 공인인증서를 사용하는 것을 권장하고 있으며, 공인인증서를 사용하는 모바일 응용 서비스의 보안성을 높이기 위한 공인인증서 관리 기법으로 임시 인증서를 활용한 기법[4], 모바일 장비에 적용 가능한 인증서 관리 시스템[1] 등의 여러 방법들이 제안되었다.

그러나 기존의 공인인증서 관리 기법들은 타인이 공인인증서의 암호를 알고 있고, 스마트폰의 공인인증서를 복제하여 사용할 경우 모든 인증절차를 통과할 수 있기 때문에 타인에 의하여 악용될 소지가 여전히 존재한다. 따라서 스마트폰의 도용이나 분실로 인한 악용은 차치하고라도, 사용자가 인식하지 못하는 사이에 스마트폰으로부터 공인인증서만을 유출하여 다른 스마트폰에서 활용하는 경우는 미연에 방지할 수 있도록 하여야 할 필요가 있다.

본 논문에서는 스마트폰 내에서 스마트폰 자체를 식별할 수 있는 IMEI와 사용자를 식별할 수 있는 IMSI를 이용하여 개인의 스마트폰과 공인인증서를 결합시킴으로써 스마트폰에서 안전하게 공인인증서를 관리, 활용하는 방안을 제안한다.

2. 관련연구

2.1 스마트폰 뱅킹

스마트폰 뱅킹이란 언제 어디서든 사용자가 스마트폰에서 인터넷 접속을 통하여 거래 은행의 잔액조회, 계좌이체, 예금조회, 환율조회, 거래내역 조회 등의 다양한 금융 서비스를 제공 받을 수 있는 것을 말한다.

작년 하반기부터 올해초까지 많은 종류의 스마트폰들이 출시되면서 스마트폰의 시장이 점차 확대되고 있다. 이처럼 스마트폰이 인기를 얻으면서 이를 통한 금융거래 즉, 스마트폰 뱅킹도 크게 증가하는 추세이다. 시중 은행들이 지난해 말부터 스마트폰을 이용한 뱅킹을 시작한 이래 한 달 동안 3만 4000여명의 사용자가 스마트폰 뱅킹 어플리케이션을 다운 받은 사례가 있으며, 스마트폰 뱅킹 서비스가 제공되기 시작한 후 현재는 많은 은행들로 스마트폰 뱅킹 서비스가 확대되고 있다. 그러나 스마트폰 뱅킹이 크게 확산되면서 이와 관련된 보안문제에 대한 우려도 커지고 있다. 이는 금융거래의 특징상 작은 보안상의 허점도 커다란 경제적 손실로 이어질 수 있다는 점 때문이다.

현재 국내의 인터넷 뱅킹 사용자는 액티브X 기반의 공인인증서를 사용하여 전자서명을 해야만 인터넷 뱅킹 서비스 및 금융 거래 서비스를 받을 수 있다. 그러나 스마트폰

은 기타 플러그인을 지원하지 않기 때문에 각 거래 은행별로 어플리케이션을 설치하고 공인인증서를 설치해야만 스마트폰 뱅킹 및 금융 거래가 가능하도록 되어 있다.[3]

2.2 스마트폰에서의 공인인증서

현재 스마트폰에서 전자금융거래를 할 때에는 전자금융감독규정 제7조에 의거해 의무적으로 공인인증서를 사용하도록 정해져 있다.[11] 그러나 공인인증서를 사용하기 위해서는 별도의 플러그인 프로그램을 설치해야 하기 때문에, 플러그인을 지원하지 않는 운영체제를 사용하는 스마트폰에서는 공인인증서 자체를 직접적으로 사용하는 것이 불가능 하다. 이 때문에 스마트폰에서 금융 거래를 하려면 각 거래 은행마다 어플리케이션의 형태로 공인인증서를 저장하고 관리를 해야만 한다.

현재 스마트폰은 IT업계에서 핫이슈로 떠오를 정도로 많은 보급이 이루어졌지만, 그에 대한 보안성은 아직 검증되지 않은 것이 많다. 스마트폰은 그 특징상 사용되는 콘텐츠의 유통이 자유롭기 때문에 온라인 구매 사이트 외에도 다양한 방법을 통해 어플리케이션을 설치하여 사용이 가능하다. 따라서 사용자가 설치한 어플리케이션에 악성코드가 포함되거나, 악의적인 의도를 가지고 만들어진 어플리케이션이 설치되면 사용자의 개인정보 유출을 통하여 금전적인 피해를 입을 수 있다. 실제로 최근에 스마트폰에서 악성코드로 인한 개인정보의 유출이나 원하지 않는 서비스를 사용한 피해 사례도 등장했다.[7] 따라서 스마트폰에서 공인인증서를 사용할 경우, 높은 수준의 보안이 이루어지지 않으면 공인인증서 정보의 유출을 통한 피해가 발생할 가능성이 높아지게 된다.

그러나 현재의 스마트폰에서 사용하는 공인인증서는 별도의 보안성을 제공하지 않는 내부 메모리나 SD메모리에 저장이 되어있기 때문에 물리적인 공격이나 악성코드로 인한 공격, 혹은 SD메모리 자체를 도용하는 등의 방법으로 공인인증서의 유출이 일어날 수 있다. 즉, 악의적인 사용자가 내부 메모리에 저장된 공인인증서를 복사하거나, 스마트폰에 장착된, 공인인증서가 들어 있는 SD 메모리 자체를 빼내어 다른 스마트폰에서 활용하는 경우가 발생할 수 있다. 그러나 현재의 금융 어플리케이션이나 공인인증서 관리 시스템은 유출된 공인인증서가 다른 스마트폰에서 사용될 때 이를 확인하여 불법적인 도용을 방지할 수 있는 장치나 시스템이 마련되어 있지 않기 때문에 도용으로 인한 피해가 발생할 가능성은 매우 높다.

3. 향상된 공인인증서 도용 방지 시스템

현재 스마트폰에서 금융 서비스를 제공하는 어플리케이션은 사용 가능한 공인인증서와 이를 식별할 수 있는 키만 있으면 인증이 가능한 구조로 시스템이 구성되어 있다.[1,2,5] 따라서 공인인증서 암호가 유출된 경우, 임의의 사용자가 공인인증서를 복제하여 사용하는 것이 얼마든지 가능하다. 물론 스마트폰 자체를 도난당하거나 분실한 경우에는 도용을 원천적으로 막을 수는 없다. 그러나 본인이 모르는 사이에 스마트폰의 인증서를 복제하거나 장착된 SD메모리를 빼내어 다른 스마트폰에서 활용하는 경우는 반드시 방지되어야 한다. 이를 위하여 본 논문에서는 타인이 공인인증서의 암호를 알고 있고, 공인인증서를 복제하여 다른 스마트폰에서 사용하고자 할 경우에, 복제되거나 도용된 공인인증서를 임의로 사용할 수 없도록 함으로써 공인인증서의 보안성을 향상시킬 수 있는 시스템을 제안한다.

3.1 IMEI와 USIM의 IMSI

WCDMA 기반의 3G 스마트폰에는 IMEI(International Mobile Equipment Identity)라고 하는 단말기 식별번호가 존재한다. 이는 각 스마트폰마다 할당되는 유일한 식별자이며 IMEI는 <표 1> 과 같이 15자리의 숫자로 구성되어 있다.[10]

<표 1> IMEI의 구조

정보	TAC	SNR	spare
크기	8bit	6bit	0 or 1bit

TAC : Type Allocation Code
SNR : Serial Number

USIM은 WCDMA 네트워크 접속 및 가입자 인증 소프트웨어 모듈로써 3G 모바일 단말에 장착되는 통신용 스마트카드인 UICC(Universal Integrated Circuit Card)에 탑재되어 구동된다. USIM 어플리케이션은 가입자 정보, 네트워크 정보, 인증 정보 등의 중요 정보와 텍스트 메시지, 이메일, 폰 북 등의 개인 부가서비스 정보를 저장한다. USIM 어플리케이션은 WCDMA 가입자 인증을 위하여 인증센터(AuC : Authentication Center)와 비밀키(K)를 공유하여 인증절차를 수행한다.

USIM 내부에는 IMSI(International Mobile Subscriber Identity)라고 하는 15자리의 가입자 식별번호가 저장 되어 있고, 서비스 개통시 사업자에 의해 부여된다. IMSI의 구성은 <표 2>와 같다.[8]

<표 2> IMSI의 구조

정보	MCC	MNC	MSIN
크기	3bit	2 or 3bit	max 10bit

MCC : Mobile Country Code
MNC : Mobile Network Code
MSIN : Mobile Subscriber Identification Number

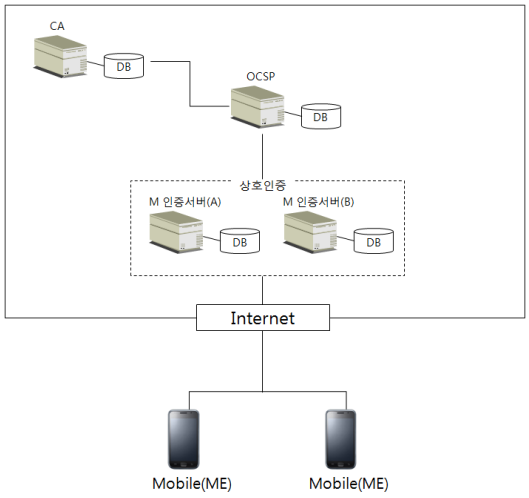
IMSI의 구성에 따라 IMSI는 3G 모바일 단말을 식별할 수 있는 유일한 키로 사용할 수 있으며, IMSI는 수정이 불가능하다. 따라서 각각의 유일한 값을 가지는 IMEI와 IMSI를 조합하여 사용하면 해당 스마트폰에 대한 유일한

값을 구성할 수 있다.

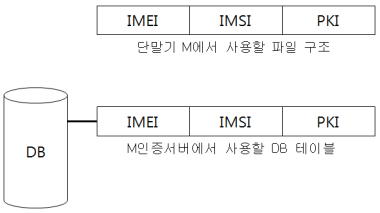
공인인증서 검증 방식으로는 OCSP(Online Certificate Status Protocol) 기반의 인증서 검증방식을 사용한다. OCSP 인증서 상태 검증방식은 클라이언트가 인증서 검증 작업을 수행하기 위한 인증서를 저장한 장소 URL에게 인증서 검증을 요청하고 그 결과만 클라이언트가 받아 작업을 수행하는 방식이다.[9] 클라이언트는 받은 인증서를 OCSP 서버에게 보내서 그 인증서의 정확성 여부를 묻게 된다. 그러면 OCSP 서버가 해당하는 인증서의 검증작업을 해서 클라이언트에게 인증서의 정확성 여부를 알려 주게 된다.[6]

3.2 제안 시스템 구성

본 논문에서 제안하는 시스템인 APS(Authenticate of PKI on Smartphone)에서는 스마트폰의 금융 어플리케이션이 사용하는 공인인증서를 내부 메모리나 SD 메모리에 저장하고, M 인증서버를 통하여 인증을 수행하도록 한다. 인증을 하기 위한 키로는 IMEI와 IMSI를 사용한다.



(그림 1) 전체구성



(그림 2) 파일구조 및 DB 테이블

(그림 1)은 이와 같은 시스템의 전체적인 구성을 나타낸다. 각 스마트폰은 인터넷을 통하여 금융 서비스 시스템인 M 인증서버로 접속을 하고, M 인증서버는 PKI의 OCSP를 통해서 사용하고 있는 공인인증서를 검증한다. 이 M 인증서버는 RA를 확장한 서버 시스템으로 IMEI와 IMSI정보를 포함하여 구현된다. 각 스마트폰 단말기는 M 인증서버의 DB와 연동하게 된다. 스마트폰에서 사용하는 정보의 파일 구조와 M 인증 서버에서 사용하는 DB 테이블의 구조는 (그림 2) 와 같으며 초기 정보 설정 단계에서 생성된다.

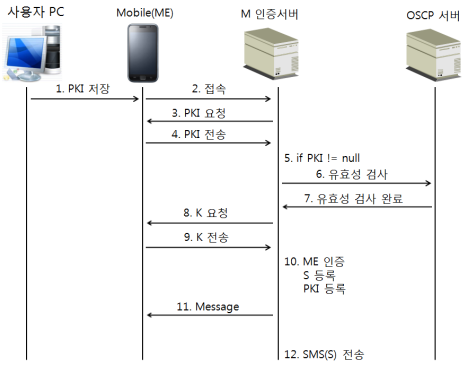
3.2.1 설정단계

설정 단계에서는 스마트폰에서 공인인증서를 사용할 수 있도록 초기 설정 작업을 하도록 한다. 초기 설정 과정에서 사용되는 요소들은 <표 3>과 같이 정의된다.

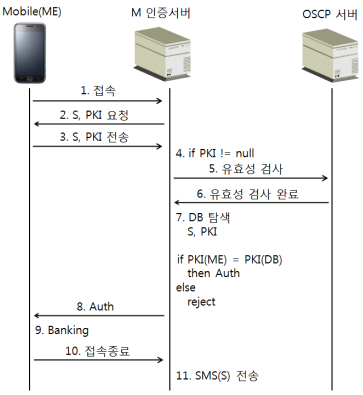
<표 3> 초기 설정 요소

S	IMEI ‖ IMSI
K	Login ID, Password, 주민등록번호, S
ME	단말기(스마트폰)
M 인증서버	단말기 인증서버

(그림 3)은 초기 등록 과정이 수행되는 절차를 나타내고 있다.



(그림 3) 초기 등록과정



(그림 4) 사용자 인증 및 실행

3.2.2 실행단계

실행단계에서는 사용자가 어플리케이션을 이용하여 단말기와 사용자 인증을 거치는 과정으로 (그림 4)의 절차를 가진다. 이와 같은 과정을 통하여 공인인증서가 특정 단말기와 연동되도록 할 수 있다. 실행 단계를 거치고 나면, 공인인증서가 유출되어도, 해당 단말기에 내장된 정보 없

이는 사용될 수 없기 때문에 공인인증서를 사용한 악의적인 응용이 실행될 수 없게 된다. 제안한 시스템은 공인인증서의 보안성을 높였고, 스마트폰에서의 공인인증서 사용에 대한 안전성을 높였다.

4. 기존의 시스템과 비교

기존의 스마트폰 뱅킹 시스템에서는 공인인증서를 다른 스마트폰으로 복사를 한 후 공인인증서의 암호만 알고 있으면 제약 없이 사용할 수 있었기 때문에, 금융 서비스를 사용시 금전적인 문제가 발생할 수 있다. 그러나 IMEI와 IMSI를 키로 사용하여 공인인증서를 관리하면, 공인인증서가 복제되거나 공인인증서 암호가 노출되는 경우 이외에 IMEI 와 IMSI 까지 노출되는 경우에도 IMSI는 수정이 불가능하기 때문에 안전할 수 있다. 즉, 인증서를 복제하거나 인증서가 들어 있는 메모리를 사용하여 다른 단말기에서 도용할 수 없기 때문에 안정성이 높다. 제안하는 시스템에서는 초기 설정 과정에서 사용자에게 등록 내용을 SMS로 전송하는 과정이 알람 역할을 한다. 따라서 공인인증서가 저장되어 있는 스마트폰을 분실하지 않는다면, 사용자는 공인인증서를 기존의 다른 공인인증서 관리 기법에 비하여 보다 안전하게 관리할 수 있다.

<표 4> 기존 기법과 제안한 기법 비교

구분	APS	Java 기반	클라우드 기반
인증서 저장위치	내부/ SD메모리	내부 메모리	클라우드내
인증서 접근방법	어플리케이션	어플리케이션	클라우드에 접속
플러그인 설치	필요	필요	필요없음
안전성을 위한 보안 요소	IMEI + IMSI + SMS	없음	SSL + OTP
단말기에 대한 공인인증서의 상관도	높음	낮음	낮음
공인인증서 관리에 대한 안전성	스마트폰과 M 인증서버의 안전성 제공	스마트폰의 안전성 제공	모바일 클라우드 서비스 업체의 안전성 제공

본 논문에서 제안된 APS 기법의 평가를 위하여 기존의 공인인증서 관리 기법과의 정성적인 비교, 분석하였다. 정성적 비교 대상으로는 Java 기반의 암호 API를 활용한 CA 및 공인인증서 관리 기법[1] 과 모바일 클라우드 기반의 관리 기법[7]의 두 가지 기법을 제안된 관리 기법과의 비교 대상으로 하였다. 주요 비교 항목으로는 공인인증서의 안전성과 안전성을 위한 보안 요소로서, 어느 기법이나 공인인증서의 암호가 이미 노출되었다고 가정하는 상황에서의 비교 결과를 나타낸다. <표 4>는 각 관리 기법들의 정성적인 비교 분석내용을 보인다.

5. 결론

본 논문에서는 스마트폰 뱅킹을 위해 IMEI와 IMSI를 키로 사용하여 공인인증서를 효과적으로 관리할 수 있는 방법을 제안하였다. 이는 기존의 시스템과 달리 개인의 등록된 스마트폰에서만 금융 서비스를 사용할 수 있고, 특정 공인인증서를 스마트폰 기반의 금융 서비스 시스템에 등록을 하고 사용하도록 함으로써, 공인인증서와 암호가 불법적으로, 또는 악의적으로 유출되었을 때 유출된 공인인증서가 본인의 스마트폰 이외의 다른 스마트폰에 복제되어 활용되는 경우를 원천적으로 봉쇄함으로써 공인인증서의 보안성을 증대시킬 수 있다. 따라서 본 논문에서 제안한 공인인증서 관리 기법은 이를 사용하는 스마트폰을 기반으로 한 금융 서비스에 대하여 기존의 공인인증서 관리 기법에 비하여 높은 보안 안전성을 제공할 수 있다.

참고문헌

[1] 김지현, 최병선, 채철주, 이재광, “모바일 장비에 적용 가능한 인증서 관리 시스템에 관한 연구”, 한국인터넷정보학회 추계학술발표대회 제7권 제2호, pp.165-168, 2006

[2] 신승수, 최승권, 조용환, “인증시간 단축을 위한 무선 PKI”, 한국콘텐츠학회 춘계 종합학술대회 논문집 제2권 제1호, pp.311-316, 2004

[3] 이경형, 김이영, “국내 은행의 모바일뱅킹 서비스 현황”, 정보통신정책 제14권 18호, 2002

[4] 이병래, 고찬, 김태윤, “임시 이동 사용자 인증서에 기반한 효율적인 인증 기법”, 한국정보과학회 가을 학술발표논문집 Vol.28, No. 2, pp.613-615, 2001

[5] 이용, 이구연, “휴대폰에서의 무선 인증서 관리 프로토콜”, 전자공학회 논문지 제45권 TC편 제10호, pp.868-876, 2008

[6] 조용환, 신승수, 최승권, 조현국, 송종명, “패스워드를 이용한 모바일 PKI 인증구조”, 정보통신기초기술연구과제, 04-기초-090, 2005

[7] 황문영, 고웅, 이동범, 곽진, “모바일 클라우드 컴퓨팅을 이용한 스마트폰 뱅킹에서 공인인증서 관리 방안”, 대한전자공학회 하계학술대회 제33권 1호, pp.1873-1876, 2010

[8] D Strobel, "IMSI Catcher", Ruhr-Universit¨at Bochum, 2007

[9] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol-OCSP", RFC2560, 1999

[10] 3GPP, Numbering addressing and identification, Technical Specification Group Core Network, 3rd Generation Partnership Project(3GPP), TS 23.003 V7.9.0, March 2009

[11] http://www.law.go.kr