모바일 기기를 이용한 인증서 관리 연구

남용수* · 김태용** · 장원태** · 이훈재**

동서대학교 유비쿼터스IT학과*, 동서대학교 컴퓨터정보공학부**

On Research of Certificates Management on Mobile Device

Yong-su Nam* · Tae Yong Kim** · Won Tae Jang** · Hun Jae Lee

Dongseo University

E-mail : virus56@nate.com* · tykimw2k@gdsu.dongseo.ac.kr

jwtway@gdsu.dongseo.ac.kr · hjlee@gdsu.dongseo.ac.kr

요 약

공인인증서는 온라인 금융거래와 증권거래 등에서 사용자의 신원 확인을 위해 사용된다. 이때 사용자의 공개키는 공인인증서에 저장되며, 이 공개키에 대응되는 사용자의 개인키는 보안을 위해 사용자가 설정하는 패스워드로 암호화 되어 개인키 저장파일에 저장된다. 본 연구에서는 로컬에서 공인인증서에 접근하는 현재의 방식에 문제점을 지적하고 이를 해결할 수 있는 방법으로 모바일 공인인증서 관리 어플리케이션을 제안한다.

ABSTRACT

Qualified certificates in online financial and security transaction area are currently used for authentication of the user. The authorized user's public key certificates are stored in binary; the private key corresponding to the user's public key certificates is encrypted by the user password, and then is stored in a file. But the present management system to access the public certificates in local has some problems. In this study, we propose that the mobile public certificate management application to avoid the exist problems.

키워드

Mobile, Bluetooth, PKI, Security

Ⅰ. 서 론

정보통신의 기술 발달로 인해 인터넷을 통한 전자 상거래나 금융 거래가 일반화 되고 있다. 하지만 이러한 서비스는 데이터의 위조와 변조, 데이터 송신 또는 수신의 부인 같은 문제가 발생할 수 있다. 이러한 문제를 해결하기 위한 방법으로 공개키 기반의 전자서명이 사용되고 있다.

전자서명 시스템에서 사용되는 공인인증서와 개인키 저장파일은 X.509 Ver3의 기준에 따라서 작성되며, BER/DER 방식으로 인코딩되어 저장된다. 공인인증서에는 사용자 공개키가 저장되며 개인키 저장파일에는 사용자의 개인키가 저장되는데, 사용자의 개인키는 다른 사용자에게 노출되면 보안상의 위험이 있으므로, SEED 블록 암호 알고리즘을 이용하여 암호화 된다. SEED 블록 암호 알고리즘에 사용되는 비밀키는 사용자의 개인키 암호화 패스워드(K_{SEED})를 이용하여 생성된다[1].

하지만 공인인증서가 로컬PC에 저장된 경우에는 공격자가 이를 취득할 수 있는 문제점이 있다. 또한 공인인증서를 사용하기위해 사용자의 개인키를 복호화 하는 과정에서 K_{SEED}를 키보드를 통해 입력받게 된다. 이것은 사용자의 부주의로 설치된 Keylogger에 의해서 공격자에게 노출 될 수 있다.

본 연구에서는 현재 사용하고 있는 공인인증서의 문제점을 지적한다. 또한 이를 해결하기 위한 방법으로 모바일 기기에 사용자의 공개키와 개인키를 저장하여 사용자가 공인인증서를 사용하기 위해 개인키를 복호화 하기 위한 K_{SEED}의 입력을 모바일 기기의 키패드를 사용하고 이를 블루투스를 사용하여 로컬PC를 통해 전송하는 인증서 관

리 프로그램 구현을 목표로 한다.

II. 기초 연구

2.1 전자서명 기술 개요

현재 인증서와 관련한 국제표준으로는 X.509 V3이 있다. 1988년 ITU-T(International Telecommunication Union Sector - Telecommuncation)에서 X.509 V1이 처음 제정되었으며, 1993년 ITU-T에서 X.509 V2가 제정되었고, 1995년 이후 ISO/IEC 9594-8문서와 동일시되어 공동 개발되고 있다. 1997년 이후 X.509 V3이 제정되어 널리 사용되고 있으며, 2000년 X.509 네 번째 판이 제정된마 있다. X.509 V2 까지 정의된 인증서 영역을 기본 영역이라 하며, X.509 V3부터 추가로 정의된 부분을 확장영역이라고 한다[3]. 다음의 표 1.과 표 2.는 인증서에 포함되는 기본필드와 황장영역의 필드의 내용을 보여준다.

표 1. 인증기관 인증서 프로파일 기본필드[2]
Table 1. CA Certificates Profile Basic Field

기본필드명	생성	처리
Version	m	m
Serial Number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m
Subject	m	m
Subject Public Key Info	m	m

표 2. 인증기관 인증서 프로파일 확장필드
Table 2. CA Certificates Profile Expand Field

확장필드명	Critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
Subject Key Identifier	n	m	m
Key Usage	c	m	m
Private Key Usage Period	n	x	x
Certificate Polices	b	m	m
Policy Mappings	n	o	m
Subject Alternative Names	n	m	m
Issuer Alternative Name	n	o	m
Subject Directory Attributes	n	x	x
Basic Constraints	c	m	m
Name Constraints	c	o	m
Policy Constraints	c	o	m
Extended Key Usage	b	o	m
CRL Distribution Points	n	m	m
Authority Infomation Access	n	o	o
Procuration	-	-	-

c : critical n : non-critical
b : critical or non-critical - : net defined
m : mandatory o : optional
x : not recommended

그림 1.은 전자 서명에 사용되는 인증 프레임 워크를 보여 준다. 사용자는 비밀키를 이용해서 CA(Certification Authority)의 인증서를 암호화 하여 전자 문서와 함께 전송한다. SP(Service Provider)측에서는 수신한 인증서를 사용자의 공개키로 복호화 하여 상위 인증기관을 확인하고 전자 문서를 신뢰할 수 있다.

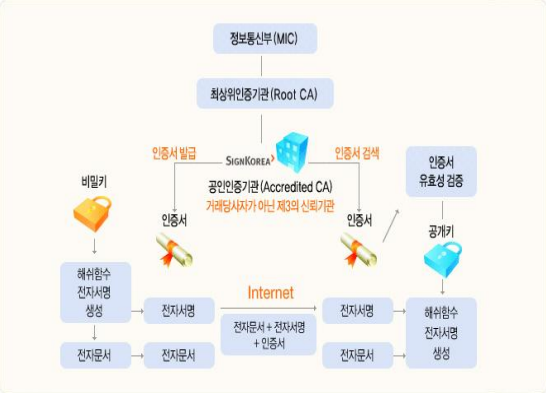

그림 1. 인증서 프레임워크
Fig 1. Certificates Framework

2.2 기존 인증서 문제점 분석

기존의 인증서는 사용자의 전자서명키를 패스워드로 암호화하여 공인인증서와 같이 하드디스크에 저장하여 사용하고 있다.

그러나 국내 전자서명 인증체계에서는 공인인증기관간 인증서 상호 연동을 위해 공인인증서 저장위치를 공개하고 있어 해커들의 표적이 되고 있다. 전자 서명키는 암호화 되어 저장되어 있지만, 키보드해킹 등으로 인해 패스워드의 획득이 가능하므로 하드디스크나 이동형 저장장치에 저장된 사용자의 공인인증서와 전자서명키는 해킹에 쉽게 노출될 수 있다[4].

또한 인증서 관리 소프트웨어를 통해 인증서를 삭제 하더라도 복구 프로그램을 이용해서 복구가 가능하고 복구된 서명파일을 통해서 사용자의 패스워드를 검출할 수 있다[4].

MITM(Man In The Middle Attack)의 문제점 또한 지적할 수 있다. 물론, MITM의 문제는 공인인증서비스 자체의 취약점에 의한 것은 아니며, 사용자의 부주의에 의해 일어나는 문제점이다.

MITM공격의 경우 그림 2와 같은 보안 경고창을 브라우저에서 출력하지만 사용자의 부주의로 "예" 버튼을 클릭하게 된다. 따라서 공격자는 사용자의 인증서를 자신의 인증서처럼 사용할 수 있게 된다.

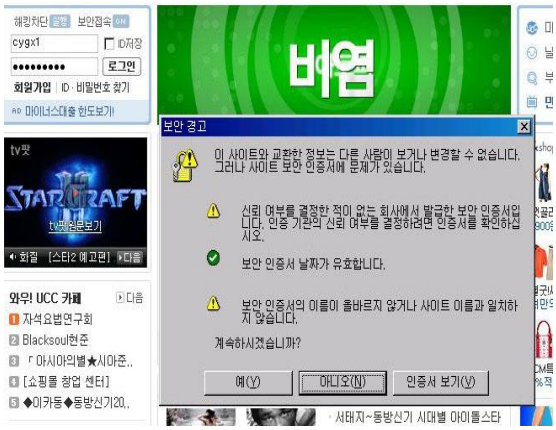

그림 2. 인증서 보안 경고
Fig 2. Certificate Security Alert

III. Mobile Certificates Profile

3.1. Mobile Certificates Profile 제안

Mobile Certificates Profile(MCP)는 사용자의 전자서명파일 패스워드를 효율적으로 관리하기 위한 방법이다. 또한 모바일 기기의 프로세서를 사용하여 SP의 인증서를 검증한다.

사용자가 SP의 홈페이지에 접속하면 블루투스를 통해 사용자의 모바일 기기로 인증서가 전송되고 모바일 기기는 전송된 인증서를 가지고 홈페이지의 신뢰성을 검증한다. SP에서 전자서명을 요청 하면 모바일 기기에 저장된 전자서명키의 패스워드를 모바일 기기의 키패드를 통해 입력받아 서명하고, 인증서와 함께 블루투스를 통해 PC에 전송한다. PC에서는 블루투스를 통해 전송받은 인증서와 전자서명 파일을 인터넷을 통해 SP에게 전송한다.

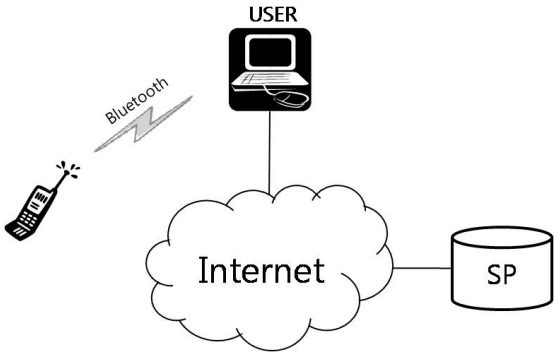

그림 3. MCP 개요도
Fig 3. MCP Overview

3.2. MCP의 데이터 플로우

그림 4는 MCP의 데이터 플로우를 보여준다. 사용자가 인증기관에 인증서를 요청하면 인증기관에서는 사용자의 Mobile 기기를 통해 사용자를 인증하고 공인인증서와 사용자의 전자서명키, 인증서 관리 프로그램을 사용자의 기기로 전송한다.

사용자가 SP에게 서비스 요청을 하면 SP는 자신의 인증서를 사용자에게 전송한다. 전송받은 인증서는 모바일 기기에 있는 인증서 관리 프로그램을 통하여 인증서 검증을 하고 시뢰할 수 있는 인증서인 경우 사용자의 전자서명 패스워드 입력을 대기한다.

사용자의 패스워드로 복호화된 전자서명키와 공인인증서를 블루투스를 통해 사용자의 PC로 전송하고 PC는 전송받은 내용을 인터넷을 통해 SP에게 전송한다.

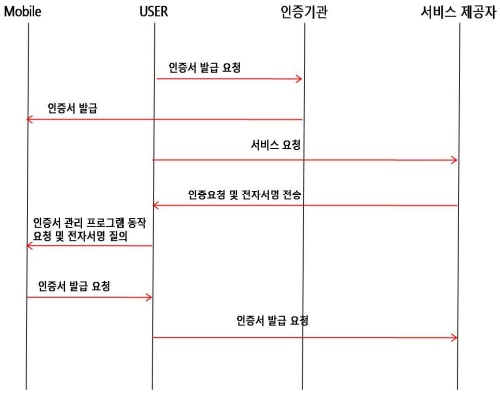

그림 4. MCP 데이터 플로우
Fig 4. MCP Data Flow

IV. 결 론

지금까지 블루투스를 탑재한 모바일 기기를 이용하여 사용자의 개인정보를 안전하게 보관하고 전송하기 위한 인증서 관리 응용프로그램을 설계하였다.

본 논문에서 제안한 MCP의 특징은 모바일 기기의 프로세서를 사용해서 피싱 싸이트의 감지와 사용자의 부주의에 의해 발생할 수 있는 MITM 공격에 효율적으로 대응할 수 있다. 또한 모바일 기기를 통해 전자서명키를 복호화 하기위한 패스워드를 입력받고, 전자서명키와 공인인증서가 저장된다. 따라서 전자서명키와 공인인증서, 사용자 패스워드가 공격자에게 유출될 위험이 적어진다.

본 설계를 바탕으로 차후 MCP의 구현을 목적으로 하며, 이 연구를 통해서 인터넷 금융거래 혹은 사용자의 인증이 필요한 서비스에 대해서 보안성을 높일 수 있을 것으로 기대된다.

참고문헌

[1] 최희봉, 오수현, 홍순좌, 원동호, “PKI 연동 키복구암호 시스템 설계에 관한 연구, 정보보호학회논문지 12(1), pp. 11-19, 2002.
[2] TTAS.KO-12.0012/R1, "전자서명 인증서 프로파일 표준“, 2006.
[3] 정연호, 최원석, 권태경, 이광수, “국내 PKI 구축현황 및 기술”, 정보보호학회지 17(6), 2007.
[4] 강신범, 정현철, “인터넷 뱅킹 해킹유형과 대응기술”, 정보보호학회지 15(4), 2005.
[5] 최윤성, 이영교, 이윤호, 박상준, 양형규, 김승주, 원동호, “삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출”, 정보보호학회 논문지 17(1), 2007