모바일 디바이스를 이용한 전자서명 서비스의 보안 위협 분석

이동범*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : dblee@sch.ac.kr, jkwak@sch.ac.kr

Security Threat Analyses of Electronic Signature Service by Mobile Device

Dongbum Lee*, Jin Kwak**
*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University
**Department of Information Security Engineering,Soonchunhyang University

요 약

공개키 암호 시스템을 이용하는 공인인증서는 IT 기술의 발달과 함께 e-Banking, e-Commerce, e-Finance 등 다양한 분야에서 사용자 인증을 제공하는 수단으로 사용되고 있다. 그러나 최근에 다양한 해킹툴과 사용자 PC의 취약점을 이용하여 PC에 저장된 공인인증서가 유출되는 사고가 발생하면서 전자금융에 대한 안전성을 위협받고 있다. 따라서 본 논문에서는 기존에 공인인증서를 하드디스크에 저장하여 발생하였던 문제점을 해결하고자 모바일 디바이스를 이용하여 전자서명을 수행하는 MobiSign의 공인인증서 이동방식 및 전자서명 방식을 분석한다. 또한 모바일 환경에서 악성코드에 의해서 발생할 수 있는 MobiSign 서비스의 보안 위협을 분석한다.

1. 서론

기본적으로 사용자의 신원을 확인하기 위한 인증은 세 가지 개념에 기반을 두고 있다. 첫째는 지식기반 인증(Something you know)으로 사용자가 알고 있는 정보를 통해 인증을 수행하는 방식이다. 대표적인 방식은 ID/PW를 통한 인증으로써 사용자가 제공한 ID/PW가 시스템에 저장되어 있는 ID/PW와 동일한지 비교하여 사용자의 인증을 수행하는 방법이다. 두 번째는 존재기반 인증(Something you are)으로 사용자의 바이오정보를 이용하여 신원 인증을 수행하는 방식이다. 대표적인 방식은 얼굴, 지문, 홍채 등 바이오정보를 내장하여 사용자 인증을 수행하는 전자여권 시스템이 있다. 마지막으로 소유기반 인증(Something you have)은 사용자가 소지한 정보를 개인 인증에 활용하는 방식으로써 대표적인 방법은 공개키 암호 시스템 기반의 공인인증서가 있다.

신원확인을 위한 세 가지 방식 중 소유기반 인증 방식의 일부인 공인인증서의 관리 프로그램에서 최근에 해킹에 이용될 수 있는 취약점이 발견되었다. 공인인증서에 대한 취약점은 아니지만 공격자가 사용자 PC의 공인인증서 관리 프로그램에서 온라인 쇼핑, 증권 거래, 금융거래를 이용할 때 ActiveX의 취약점을 이용하여 악성코드를 설치하고 사용자 PC의 제어권한을 획득한 후 데이터를 절취하는 문제점이 발생하였다[3].

따라서 본 논문에서는 기존에 공인인증서를 하드디스크에 저장하여 발생하였던 문제점을 해결하고자 공인인증서를 모바일 디바이스로 이동/저장하고 모바일 디바이스 내에서 직접 전자서명을 수행할 수 있는 MobiSign 서비스를 분석하고자 한다.

본 논문의 2장에서는 MobiSign의 공인인증서 이동방식 및 전자서명 방식을 분석하고, 3장에서는 모바일 디바이스를 이용하는 MobiSign에서 발생할 수 있는 보안 위협을 분석한다. 마지막으로 4장에서 결론을 맺는다.

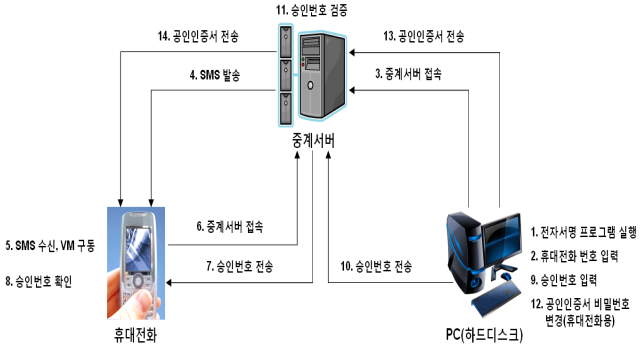
2. MobiSign 개요

MobiSign은 모바일 디바이스를 이용한 전자서명 서비스로써 하드디스크에 저장되어 있는 공인인증서를 모바일 디바이스로 이동/저장하고 모바일 디바이스 내에서 직접 전자서명을 수행할 수 있다. 인증서 이동 및 전자서명을 수행하는 일련의 과정은 모바일 디바이스에 설치되는 MobiSign VM(Virtual Machine)을 통해 수행되고, 인증서 및 전자서명값은 중계서버를 통해 이동된다. 특히, MobiSign은 PC방, 원격접속 등 보안이 안전하지 않은 PC 환경에서도 안전하게 전자서명을 수행할 수 장점을 가지고 있다[1].

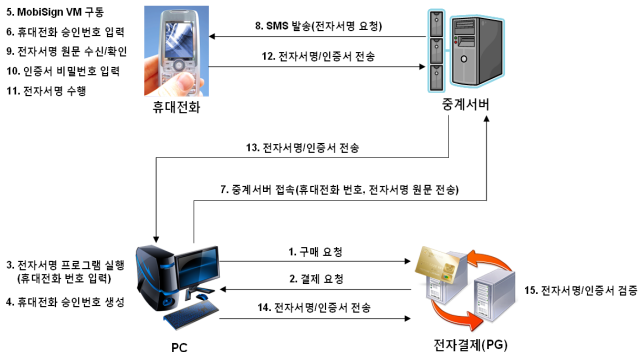
2.1 MobiSign 프로세스

<그림 1>은 MobiSign을 이용하여 PC에 저장된 공인인증서를 모바일 디바이스로 이동하는 과정을 나타내고,

<그림 2>는 MobiSign에서 전자서명을 수행하는 과정을 나타낸다.



<그림 1> MobiSign의 공인인증서 이동 방식



<그림 2> MobiSign을 이용한 전자서명 방식

3. MobiSign 보안 위협

공격자는 불법적인 접근을 시도하거나 비정상적인 방법으로 MobiSign 서비스에 대하여 악의적인 공격을 수행할 수 있다. 공격자는 바이러스, 웜, 트로이목마, 스파이웨어와 같은 다양한 형태와 기술적인 방법으로 MobiSign 서비스의 가용성을 방해할 수 있으며, 피싱 사이트와 같은 사회공학적 해킹과 모바일 디바이스의 하드웨어/소프트웨어의 취약점을 이용하여 공격할 수 있다.

<표 1>은 MobiSign에 수행될 수 있는 공격 방법을 나타내고, <표 2>는 공격자가 MobiSign의 공격에 이용될 수 있는 악성코드를 분석한 결과를 나타낸다[2][4].

<표 1> MobiSign 공격 방법

공격 방법	설명
MobiSign 공인인증서 유출	· 블루투스의 무선 통신을 이용한 공인인증서 유출 · MMS를 이용한 공인인증서 유출 · CxOver 웜과 같이 이종 디바이스를 이용한 공인인증서 유출
MobiSign 서비스 방해	· SMS/MMS를 이용한 DOS 공격 · MobiSign 공인인증서의 저장 공간을 0Kbyte로 변경 · MobiSign의 실행 아이콘을 변경/삭제
MobiSign VM 공격	· MobiSign VM의 실행 파일을 변경/삭제 · MobiSign VM의 오작동 유발
MobiSign 피싱 사이트	· MobiSign 사이트를 가장한 피싱 사이트 개설 · 공격자가 개발한 위장 프로그램 업로드
MobiSign 공인인증서 추출	· 하드웨어적인 공격 수행 · 모바일 디바이스의 낸드플래시/USIM 칩에 저장된 공인인증서 추출

<표 2> 모바일 악성코드 분석

악성코드명	형태	설명
WinCE.Duts	바이러스	· 최초로 Windows CE.NET에서 감염된 바이러스 · ARM 프로세서의 실행파일을 감염시킴
FlexiSpy	스파이웨어	· 최초의 상용 스파이웨어 · 사용자의 전화번호/통화내역/SMS을 수집하여 원격서버로 전송/감시
Cabir	웜	· 블루투스의 기능을 이용하여 전파되는 최초의 웜
Commwarrior	웜	· 휴대전화의 서비스 기능과 융합 · 블루투스/MMS 기능을 이용하여 휴대전화에 저장된 주소록을 발송/전파
Lasco	웜	· 블루투스 기능을 통해 복제 · SIS 파일이 감염된 장치에 전파
CxOver	웜	· 최초로 이종 디바이스(PC, PDA)간 교차 감염되는 악성코드 · 마이크로소프트의 ActiveSync를 실행할 때 감염시킴
Skulls	트로이목마	· 아이콘을 모두 해골모양으로 변경/삭제 · 프로그램 다운로드 설치시 감염시킴 · 프로그램 실행 방해
Hobbes	트로이목마	· 안티바이러스를 가장한 최초의 트로이목마 · 파일 다운/메일을 확인할 때 감염시킴 · 전화 송/수신만 가능하고 다른 기능들은 사용 불능하게 만듦
Cardtrap	트로이목마	· PC를 공격하는 최초의 트로이목마 · 휴대전화의 메모리 카드에 Win32/Padobot.Z, Win32/Rays 웜을 감염시킴 · 감염된 메모리 카드를 PC에서 사용할 때 윈도우를 감염시킴
PbStealer	트로이목마	· 유틸 프로그램으로 가장하여 감염시킴 · 사용자의 휴대전화에 저장된 주소록 정보를 유출시킴
RedBrower	트로이목마	· 최초로 J2ME 기반의 JAVA 코드로 작성된 악성코드 · WAP 브라우저로 가장하여 설치되며, 특정 번호로 SMS 발송
Fontal	트로이목마	· 블루투스를 이용하여 감염된 파일을 전송 · 거짓 오류 메시지 출력/휴대전화 부팅 방해

4. 결론

모바일 디바이스는 기존의 음성 통화 기능과 MMS 서비스뿐만 아니라 멀티미디어, 인터넷, 전자 결제까지 다양한 기능을 갖춘 스마트폰 형태로 발전하고 있다. 즉 기존의 PC에서 사용하던 유선 네트워크 환경에서의 여러 보안 위협들이 모바일 디바이스에서 발생할 수 있다. 따라서 모바일 디바이스를 이용하는 MobiSign 서비스의 안전성을 높이기 위해서는 모바일 전용 백신을 개발하고, 새로운 보안 위협에 대한 분석이 필요하다.

참고문헌

[1] http://www.mobisign.kr
[2] http://www.symantec.com
[3] 이원철, 이석래 외 "전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구" 정보보호학회지, 제 15권 제 4호, pp. 43~48, 2005.08
[4] Steven Furnell, "Handheld hazards: The rise of malware on mobile devices", Computer Fraud & Security, Volume 2005,Issue 5, May 2005, Pages 4-8.