개인키 불법 유출 방지 및 로밍을 위한 로밍 키 관리 시스템

이평수*, 이민수*, 송오영*, 박세현*

중앙대학교, 전자전기공학부*

A Roaming Key Management System against Private Key Hijacking

Pyoung Su Lee*, Min Su Lee*, Oh Yung Song*, Se Hyun Park*

School of Electronic and Electrical Engineering, Chung-Ang University*

요 약

본 논문에서는 현재 국내·외에서 개발되고 있고 이미 상용화가 되어 있는 PKI 기반 인증 시스템에서 개인키의 로밍을 구현하고 특정 개인 컴퓨터에 개인키가 보관 되어있을 경우 발생할 수 있는 개인키의 불법 유출의 위험을 방지 할 수 있는 Roaming Key Management System의 개발 및 방안 연구를 목적으로 한다. RKMS 는 사용자의 인증서와 개인키를 개인 컴퓨터에 보관하지 않고 신뢰 할 수 있는 키서버에 저장함으로써 개인키 불법 유출을 막을 수 있고 개인키 로밍을 가능하게 한다. RKMS는 현재 발생되어 지고 앞으로 발생될 것으로 예상되어지는 인증서 및 개인키 해킹의 대안의 방법으로 사용되어 질 수 있다. 이를 이용하여 PKI 기반 인증 시스템의 향상된 안정성과 편리성을 구현하고 개인키 누출을 방지할 수 있다.

I. 서론

네트워크의 발달과 함께 인터넷을 이용한 부가적인 서비스들이 속속 등장하고 있다. 인터넷 쇼핑, 게임, 그리고 증권 및 인터넷 뱅킹과 같은 서비스들이 계속 개발되고 또 운영되고 있다. 이러한 인터넷 서비스에서 인증부분은 중요한 비중을 차지하고 있다. 인증이 제대로 되어야만 사용자에게 올바른 권한을 부여하고 서비스를 할 수 있다. 인증 방법중 인증서[1]를 이용한 인증방법이 현재 많이 사용되어지고 강력한 인증을 수행하고 있다. 인증서를 사용한 대표적인 인터넷 서비스로는 인터넷 뱅킹[4]을 들 수 있다. 또한 정부는 인증서를 이용한 전자 정부 서비스를 부분적으로 시작하고 있으며 점차 서비스 영역을 확대시켜 나갈 전망이다. 그런데 인증서를 이용한 인증에서의 문제점은 인증서를 통한 인증 효력이 강력하기 때문에 이러한 인증 과정에서 개인키[2] 누출이 발생했을 경우 막대한 경제적 손실을 가져올 수 있다는 것이다. 또한 개인키가 유출되어 현재 불법적인 사용이 이루어지고 있음에도 개인키의 소유자는 현재 불법적인 용도로 개인키가 사용되어지고 있다는 사실을 인지하는데 상당한 시간이 소요될 수 있다는 문제점도 있다. 그리고 이러한 불법적인 시도로 인하여 피해가 발생하였을 경우 피해에 대한 책임소재가 불분명 할 수 있다. 그리므로 본 논문에서는 인증서를 사용한 인증 과정중 발생할 수 있는 문제점을 살펴보고 문제점 해결 방안 모델로서 개인키의 안전한 사용과 개인키가 사용되어지고 있는 상황을 사용자가 확인할 수 있는 RKMS(Roaming Key Management System) 모델을 제안한다.

II. RKMS 기반의 개인키 관리

1. 현행 인증서 관리 체계

현재 인터넷 뱅킹에서 사용되고 있는 인증서와 개인키는 해당 인터넷 뱅킹 홈페이지에서 인증서와 개인키를 발급 받아 플로피 디스켓이나 하드디스크 또는 스마트 카드[3] 등에 저장하여 사용하게 된다. 일반적으로 컴퓨터에 저장하여 사용하는 경우가 많고 또 하드디스크에 저장하는 것이 안전하다는 권장사항도 표시하는 경우가 있어서 하드디스크에 저장하여 사용하는 게 일반적인 상황이다. 또한 플로피 디스켓이나 스마트 카드에

저장하는 경우에도 하드디스크에 백업 해놓은 경우도 많다. 이렇게 하드디스크에 저장되어 있는 인증서와 개인키는 불법적인 파일 전송을 통해서 외부로 유출될 위험이 많다.

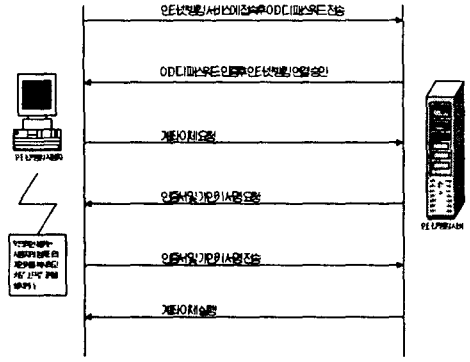

그림 1 개인키 누출 과정 예

불법적인 파일전송은 직접적인 방법으로는 해당 인증서와 개인키를 복사하여 외부로 유출하는 방법이 있고 간접적인 방법으로는 해킹툴이나 직접 작성된 파일 전송 프로그램 등으로 특정 컴퓨터로 해당 파일을 전송시키는 방법이 있다. 물론 개인키는 사용자만이 알 수 있는 특정한 암호로 암호화가 되어 있으나 악의적인 사용자의 시도로 개인키 암호는 노출되어질 수 있다. 구체적인 예로는 해킹툴을 통한 키보드 타이핑 캡처나 직접 작성한 키로그 프로그램 등으로 패스워드까지 노출될 수 있다. 그림 1은 인터넷 뱅킹 사용자의 개인키 누출과 아이디 및 비밀번호 누출의 예이다. 일반적으로 사용자의 컴퓨터에서 인터넷 뱅킹 서버로 가는 중의 데이터는 암호화가 되어 악의적인 사용자의 해킹 시도로 아이디나 비밀번호가 노출될 위험은 없다. 하지만 해커의 특정 방법으로 사용자의 컴퓨터에 특정 소프트웨어가 설치될 경우에는 아이디 비밀번호와 개인키 파일이 노출될 수 있다.

2. 현행 인증서 관리 체계의 취약점

일반적으로 인증서와 개인키는 금융 거래나 전자 입찰 등의 중요한 업무에 사용되고 있다. 인증서와 개인키의 사용은 인감증명과 비교될 만큼 강력한 효력이 있다. 이러한 중요한 개인키를 외부의 노출에 방치되도록 그냥 하드디스크에 저장한다는 것은 심각한 위험을 초래할 수 있다. 또한 유출된 개인키는 타인에 의해 인터넷 뱅킹 등과 같은 금융 서비스에 사용된다 하더라도 사용자는 현재 개인키가 사용되어지는 상황을 전혀 인지하지 못할 것이다. 그리므로 인증서와 개인키가 불법적으로 사용되어질 경우 사용자는 최대한 빨리 인증서가 사용되어지고 있음을 알 수 있어야 한다.

인증서 저장 매체 \ 특징	휴대성	경제성	안정성
하드디스크	X	O	O
플로피 디스크	O	O	X
USB 토큰	O	△	O
스마트 카드	O	X	O

표 1 현행 인증서 저장 매체 특징

또한 현행 인증서 관리 체계에서는 사용자가 외부에서 인증서를 사용하기 위해서는 스마트 카드와 같은 부가적인 수단이 필요하게 된다. 그렇지 않으면 인증서를 재발급을 받아서 사용을 하게 되는데 이는 보안에 취약한 약점을 가지고 있다. 인증서를 재발급 받기 위해서 여러 복잡한 절차를 거쳐야 하는 어려움도 있다. 표 1에서 현행 인증서 저장 매체의 특징을 설명하였다. 가장 선호되고 있는 하드디스크는 안정적이고 부가 장비가 필요하지 않아 경제적인 반면에 휴대하기가 불편하다. 플로피 디스크는 휴대하기가 용이하고 경제적인 반면에 디스크가 손상되어 개인키를 손실할 위험이 있다. USB 토큰의 경우는 휴대하기가 쉬우며 안정적이고 가격도 저렴하여서 앞으로 많이 사용될 전망이다. 스마트 카드는 휴대하기 쉽고 안정적이나 리더기를 따로 구매하여야 하기 때문에 아직 많이 사용되고 있지는 않다.

3. 서버기반의 RKMS

본 논문에서는 현행 인증서 관리체계의 문제점을 효과적으로 보완하기 위한 키 관리 시스템을 설계하여 안전한 인증서 사용과 키로밍을 가능하도록 하였다. 현행 인증서 관리 체계에서 인증서 및 개인키가 가장 많이 사용되어지는 하드디스크에 저장되어 있을 경우 해킹툴을 사용한 해커에 의해서 해킹되어 질 수 있다.

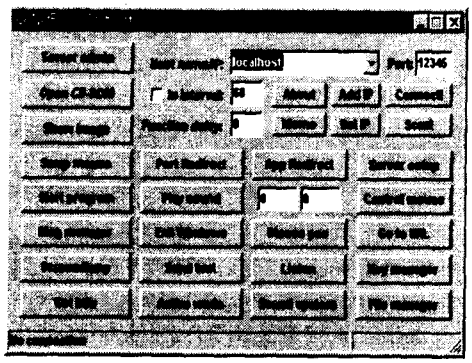

그림 2 Netbus 실행 화면

개인키 및 개인키 암호의 hijacking 은 Netbus 와 같은 해킹툴이 사용되어 지고 있다. Netbus 는 쉽게 구할 수 있고 초보 사용자들도 쉽게 사용할 수 있어 널리 이용되어 지고 있다. 그림 2는 개인키 및 개인키 암호의 해킹에 사용되는 Netbus의 실행 화면이다. 그림 2의 Netbus 실행 화면을 보면 Netbus 의 여러 기능 버튼이 있다. 이중 File manager 와 Listen 기능을 이용하면 개인키 파일과 개인키 암호를 해킹할 수 있다. Netbus Server 프로그램은 이메일이나 첨부 파일 형식으로 전파되고 있다. 일단 Netbus Server 프로그램이 설치되게 되면 해커는 File manager를 이용하여 개인키 소유자의 인증서와 개인키 파일을 다운받을 수 있다. 그리고 Listen을 이용하여 개인키 소유자가 키보드로 타이핑하는 것을 모두 캡쳐 할 수 있다. 이로서 개인키와 개인키 암호는 쉽게 노출되고 해커는 불법적인 목적으로 개인키를 사용하게 된다. 이에 비해 본 논문에서 제안한 RKMS의 경우에는 기존 해킹 방법을 통해서 시스템을 해킹할 수 없다. 그림 3은 RKMS 의 기본 동작 개요를 설명한다.

인터넷 뱅킹 서버에 접속하여 계좌 이체와 같은 서비스를 받는 과정을 살펴보면 먼저 웹 브라우저로 인터넷 뱅킹 서버에 접속을 한다. 그리고 기존의 접속방법과 동일한 방법으로 단말기의 웹 브라우저에 자신의 계정, 암호를 입력한다. 인터넷 뱅킹 서버에 접속 후 계좌 이체 서비스를 요청할 경우 인터넷 뱅킹 서버는 사용자의 인증을 위해 개인키로 서명할 것을 요청하게 된다. 이때 인터넷 뱅킹 서버는 키서버의 정보를 사용자에게 전송을 한다. 사용자는 전송 받은 키 관리 서버에 접속을 하여 다시 한번 로그인을 거치고 핸드폰 문자 메시지와 같은 Out of Band 로 전송되어지는 Token 을 전송 받게 된다. 전송 받은 Token 을 입력하면 키 관리 서버는 토큰 확인 후 웹을 통하여 사용자 인증 허가 메시지를 인터넷 뱅킹 서버에 전송한다. 이로서 계좌 이체 서비스가 완료가 된다. 기존의 해킹은 사용자 컴퓨터에 인증서 및 개인키가 보관되어 있어야 개인키 해킹이

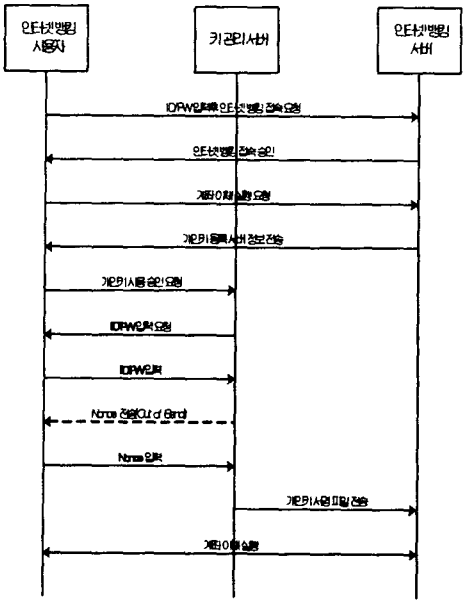

그림 3 서버 기반의 RKMS 동작 개요

가능하였고 키로그를 통하여 해당 시스템의 아이디 패스워드를 해킹할 수 있었다. 하지만 RKMS 는 사용자의 컴퓨터에 개인키가 보관되어 있지 않고 신뢰할 수 있는 키 관리 서버에 개인키를 보관하기 때문에 개인 사용자 컴퓨터의 취약점을 이용한 해킹의 위험이 없다. 또한 키로그 해킹을 방지하기 위하여 아이디 패스워드 외에 Out of Band 로 Nonce를 전송하여 사용자를 인증하는 방법을 추가하여 키로그를 통한 해킹을 방지 할 수 있다. 또한 개인키가 하드디스크에 저장되어 있는 경우에는 사용자가 장소를 변경하여 사용할 경우 재발급의 절차를 거쳐야 한다. RKMS의 경우는 인증서와 개인키가 웹으로 접근 할 수 있는 키서버에 보관되어 있기 때문에 특정 컴퓨터에 종속적이지 않고 어느 장소에서나 개인키의 유출 위험이 없이 인터넷 뱅킹과 같은 중요한 서비스를 이용할 수 있게 된다. 그리고 로밍을 위해서 스마트 카드 리더기와 같은 부가적인 장비를 필요로 하지 않는다.

항목 / 특징	기존의 개인키 및 인증서 관리	RKMS 방식의 개인키 및 인증서 관리
이동성	X	O
개인키 유출 위험	O	X
키로밍시 부가장비 필요	O	X

표 2 인증서 및 개인키 관리 체계 비교

표 2 는 기존의 개인키 및 인증서 관리와 RKMS 방식의 개인키 및 인증서 관리의 특징을 비교한 것이다. RKMS 방식의 개인키 관리 시스템의 특징을 살펴보면 이동성이 보장되어 지고 개인키 유출 위험이 없이 개인키를 언제 어디서나 사용할 수 있다.

III. 결론 및 향후 연구 방향

앞으로 정부의 전자 정부 서비스 및 민간 업체의 인증서 활성화 정책을 통하여 인증서와 개인키를 통한 많은 서비스들이 등장하게 될 것이다. 이러한 서비스들을 통하여 사용자는 좀더 편리하고 안전하게 많은 일들을 수행할 수 있을 것이다. 하지만 온라인 상에서 많은 일들을 처리할 수 있는 만큼 해킹의 위험도 또한 증대 될 것이다. 이러한 때일수록 안전한 인증 관리 정책이 요구되어 지고 인증서 보안이 더욱 필요하다. 이에 본 논문에서는 안전한 인증서 관리 및 사용을 위한 로밍 키서버를 이용한 RKMS(Roaming Key Management System)를 제안하였다. RKMS는 현재 발생되어 지고 앞으로 발생될 것으로 예상되어지는 인증서 및 개인키 해킹의 대안의 방법으로 사용되어 질 수 있다.

본 시스템의 경우는 키 관리 서버는 보안적으로 안전하다는 가정 하에 시스템을 제안하였다. 하지만 키 관리 서버의 보안이 확실하지 않을 경우 많은 사용자의 개인키가 누출될 수 있는 심각한 문제가 초래될 수 있다. 그리므로 개인키의 분산 처리 및 암호화를 통하여 개인키 저장을 보완하는 연구가 필요하다.

참고문헌

[1] ITU-T Recommendation X.509, "Information technology - Open systems interconnection - The directory : public-key and attribute certificate frameworks", 2000

[2] Nechvatal, J. "Public Key Cryptography," in [SIMM 92a]

[3] Won Jay Song, Byung Ha Ahn, "PKI-based security and privacy controls using synchronized 2-way double-type smartcard terminals for healthcare information access", Consumer Electronics, 2002. ICCE. 2002 Digest of Technical Papers. International Conference on , 2002

[4] Internet-the future delivery channel for banking services Yan, G.; Paradi, J.C. System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on , Volume: 4 , 1998