보안공학연구논문지 *Journal of Security Engineering*
Vol.11, No.4 (2014), pp.273-286
http://dx.doi.org/10.14257/jse.2014.08.01

자체확장인증과 하드웨어보안모듈을 이용한 하이브리드 키관리

이병천[1)]

Hybrid Key Management Using Self-Extended Certification and Hardware Security Module

Byoungcheon Lee[1)]

요 약

개인이 복수의 컴퓨팅 기기들을 사용하게 되는 유비쿼터스 환경에서는 인증키를 발급받고, 이용하고, 안전하게 관리하는 것이 매우 어려운 문제이다. 하나의 인증키를 여러 기기에서 복사하여 사용하거나, 기기별로 별도의 인증키를 발급받아 사용하는 방법 모두 키관리에 많은 어려움을 내포하고 있다. 한편 최근에는 안전한 키관리 도구로서 하드웨어보안토큰을 활용할 수 있는 환경이 확대되고 있는데 이들을 적극 활용할 수 있는 키관리 방안이 필요하다. 이 논문에서는 개인이 소유한 하나의 인증키를 기반으로 복수의 개인 소유 기기들에서 생성된 암호키에 대해 인증을 자체 확장하여 이용할 수 있도록 하는 통합적인 키관리 체계인 하이브리드 키관리 방식을 제안한다. 아울러 이러한 통합 키관리 시스템의 특징과 효율성을 분석한다.

핵심어 : 하이브리드, 키관리, 하드웨어보안모듈, 자체확장인증, 유비쿼터스 컴퓨팅

Abstract

In ubiquitous computing environment where users own and use multiple computing devices it is difficult for users to manage certified keys securely in multiple devices. Users can try to copy and share a single certificate in multiple devices, or have independent certificates issued in every devices, but both approaches have many difficulties in secure key management. Recently it becomes more and more common that hardware security modules are available in computing devices as secure key management devices, thus we need to have secure key management architecture to utilize them. In this paper we propose a hybrid key management system in which user owns a single certificate and self-extends certification to issue multiple extended certified keys in each device. We analyze its useful features and efficiency.

Keywords : hybrid, key management, hardware security module, self-extended certification, ubiquitous computing

접수일(2014년06월05일), 심사의뢰일(2014년06월06일), 심사완료일(1차:2014년06월20일)
게재일(2014년08월31일)

[1]312-702 충청남도 금산군 추부면 마전리 중부대학교 정보보호학과.
email: sultan@jbm.ac.kr

ISSN: 1738-7531 JSE
Copyright ⓒ 2014 SERSC

1. 서론

1.1 유비쿼터스 환경에서의 키관리

개인이 복수의 컴퓨팅 기기들을 소유하고 사용하게 되는 유비쿼터스 환경을 고려해보자. 이러한 기기들에서 개인이 인증키를 사용할 수 있기 위해서는 인증기관으로부터 인증서를 발급받아 사용하는 것이 일반적인 접근방법인데 개인이 복수의 컴퓨팅 기기들을 사용하는 경우 기기별로 인증을 어떻게 제공할 것인지를 고려해보아야 한다. 대표적으로 다음의 두가지 방법을 비교해보자.

첫째, 하나의 인증키를 여러 기기들에 복사·공유하여 사용하는 방법이 있을 수 있다. 그런데 이 방법은 비밀키가 기기 외부로 복사되고 통신을 통해 전달되며 컴퓨터의 메모리에 로드되어 관리되므로 공격자에게 탈취될 수 있는 위험이 있다. 또한 이 방식은 하나의 기기에서 비밀키가 공격자에게 탈취되는 경우 다른 모든 기기에서도 그 키를 사용할 수 없게 된다는 문제가 있다. 만일 비밀키를 외부로 복사해낼 수 없는 하드웨어보안토큰에서 생성된 키쌍에 대해 인증서를 발급받은 경우에는 비밀키를 하드웨어 외부로 복사할 수 없으므로 다른 기기에 복사하여 사용하는 방식 자체를 적용할 수 없다는 근본적인 문제점이 있다.

둘째, 각 기기별로 별도의 인증키를 발급받아서 사용하는 방법이 있을 수 있다. 이 경우 개인 사용자는 기기별로 인증서를 발급받기 위해 인증서 발급 프로세스에 여러 번 관여해야 하는 문제점이 있다. 또한 발급된 여러 개의 인증키와 이들이 저장된 기기들을 모두 개별적으로 안전하게 관리해야 하는데 사용하는 기기의 수가 증가할수록 인간에게 이것은 매우 어려운 문제가 된다.

현재까지는 개인이 복수의 컴퓨팅 기기들을 사용하게 되는 유비쿼터스 환경에서 인증키 관리를 효율적으로 수행할 수 있는 체계적인 방안이 제시되지 못하고 있다. 개인 소유의 컴퓨팅 기기들에 대해서는 외부기관에 의존하는 경직되고 복잡한 키관리보다는 개인이 직접 관리할 수 있도록 하는 키관리의 개인화가 필요하다.

1.2 하드웨어보안모듈의 이용 환경 확대

최근 안전한 키관리 도구로서 하드웨어보안모듈을 활용할 수 있는 환경이 크게 확대되고 있다. 요즘 발매되는 최신형 컴퓨터들은 메인보드에 하드웨어 기반의 보안칩인 신뢰플랫폼모듈(Trusted Platform Module, TPM)[1-3]이 장착된 형태로 출시되고 있다. 스마트폰, 태블릿컴퓨터 등의 이동통신 단말기들은 통신회사에서 가입자 관리를 위해 이용하는 범용가입자식별모듈인 USIM(Universal Subscriber Identity Module)을 장착하여 사용하게 되는데 USIM은 키관리 뿐만 아니라 여러 가지 보안기능을 구현하는데 활용될 수 있다. 최근에는 근거리 통신 기능과 보안기능이 결합된 NFC(Near Field Communication)[4-6] 칩이 내장된 스마트폰의 보급이 확대되고 있다. 또한 국내에

 Copyright ⓒ 2014 SERSC

서는 USB 형태의 인터페이스에 스마트카드칩이 내장된 형태인 USB 보안토큰을 공인인증서의 안전한 저장장치로서 널리 보급하기 위해 노력하고 있다.

이러한 하드웨어 보안모듈들은 암호키의 안전한 저장소로서의 역할뿐만 아니라 RSA기반의 키생성, 암호화, 전자서명, 해쉬, 난수생성 등의 기본 보안기능들을 가지고 있어서 비밀키의 외부 누출이 없이 암호화, 전자서명 등의 보안기능을 하드웨어보안모듈 내부에서 수행할 수 있도록 하는 안전한 사용환경을 제공한다.

1.3 공인인증 시스템 고도화

현재 국내의 공인인증 시스템에 대해 많은 비판들이 존재하는데 주된 비판 요소는 액티브엑스와 같은 비표준 부가프로그램을 브라우저에 설치해야 한다는 점, 특정 브라우저에 종속된다는 점과 더불어 컴퓨터 내부에 비밀키를 안전하게 보관하고 사용하기 어려워 각종 해킹공격에 취약하다는 점 때문이다. 국내에서는 이를 극복하기 위하여 USB형태의 보안토큰에 인증서를 저장하여 사용할 것을 권고하고 있다. USB 보안토큰을 가진 컴퓨터는 비밀키의 안전한 보관과 사용이 가능하고 암호기능 사용을 위한 부가프로그램 설치가 필요 없어서 공인인증체계의 고도화에 큰 도움이 될 것으로 예상된다.

그러나 현재까지는 USB 보안토큰이 기존 공인인증체계의 고도화 측면에서 기존에 발급받은 인증서를 안전하게 저장하고 사용하기 위한 역할로 주로 이용되고 있다. 사용자가 복수의 컴퓨팅기기들을 사용하는 유비쿼터스 환경에서의 각 기기별 인증키 관리 문제는 고려되지 못하고 있다.

1.4 인증의 자체확장 기법

이 논문에서는 하나의 인증키에 기반하여 복수개의 인증키를 사용자 스스로 유도, 확장하여 사용하는 방식을 제안하고자 하는데, 이런 개념은 인간에게 매우 상식적이고 친숙한 개념이다. 암호학적으로는 대리서명에서 비슷한 개념을 찾아볼 수 있다. 대리서명이란 한 사용자(원서명자)가 다른 사용자(대리서명자)에게 서명기능을 위임하는 방식으로서 원서명자의 키를 직접 제공하거나, 위임사항을 확인할 수 있는 특별한 키를 생성하여 사용하거나, 위임 내용을 서명된 문서로 제공하는 등의 방식으로 사용할 수 있다[7]. 이러한 방식을 이용하면 원서명자의 서명권한을 대리서명자가 대신할 수 있도록 위임할 수 있게 된다. 대리서명의 변형된 방식으로는 한 사용자가 자기자신이 사용할 목적으로 자기 자신에게 위임하는 방식이 있을 수 있다[8]. 즉, 새롭게 생성된 키들에게 스스로 위임을 생성하여 인증키로 사용하는 것이다. 이 논문에서는 이러한 인증의 자체확장 방식을 개인의 키관리에 적용하려는 것이다.

1.5 이 논문의 기여

Copyright ⓒ 2014 SERSC

개인이 소유하는 하드웨어보안모듈의 내부에서 생성되고 관리되는 암호키는 밖으로 꺼낼 수 없는 안전한 암호키이며 이것을 사용자의 인증키로 활용할 수 있도록 하는 방안이 필요하다. 이 논문에서는 개인이 인증기관으로부터 하나의 인증서를 발급받았다고 가정하고 이를 기반으로 개인이 소유한 컴퓨팅기기들에서 하드웨어보안모듈을 이용하여 안전한 암호키를 생성하고 이들에게 인증을 자체확장하여 새로운 인증키로 이용할 수 있도록 하는 하이브리드 키관리 방안을 제시하고 이것의 효용성을 보이고자 한다.

1.6 논문의 구성

2장에서는 현재 활용 가능한 하드웨어 보안모듈의 적용 현황을 살펴본다. 3장에서는 제안된 하이브리드 키관리 방식을 제시하고 4장에서는 제안 시스템의 안전성 및 효율성을 분석한다. 5장에서는 결론 및 향후 연구과제를 제시한다.

2. 하드웨어보안모듈

현재의 컴퓨팅 환경과 인터넷 통신 환경은 다양한 해킹공격에 취약성을 가지고 있어서 표준 운영체제에서 동작하는 소프트웨어만으로는 이러한 공격에 대응하기 어렵다. 이를 극복하기 위해 별도의 운영체제와 제한된 통신기능을 가지며 조작방지(Tamper proof) 기능을 가지는 하드웨어보안모듈을 함께 사용함으로써 보안기능을 구현하려는 노력이 이루어지고 있다. 현재의 컴퓨팅 환경에서는 다음과 같은 하드웨어보안모듈들의 사용이 고려될 수 있다.

2.1 신뢰플랫폼모듈(TPM)

현재의 컴퓨팅 환경과 인터넷 통신 환경은 다양한 해킹공격에 취약성을 가지고 있어서 컴퓨터가 당초 의도된 대로 동작하고 있다는 것을 보증하기 어려운 환경이다. 신뢰플랫폼모듈(Trusted Platform Module)[2-3]은 컴퓨터 메인보드에 장착되어 사용되는 하드웨어 보안칩을 말하는데 드라이브 암호화, 시스템의 무결성 보장 등을 위해 주로 사용된다. 신뢰컴퓨팅기술이란 컴퓨터가 당초 의도된 대로 동작하고 있다는 것을 보증하는 신뢰성을 부과하기 위한 것으로서 하드웨어 기반의 보안칩을 모든 기기들에 공통적으로 적용하도록 하고 이를 위한 소프트웨어를 개방형 표준으로 제공하고자 하는 기술로서 신뢰컴퓨팅그룹(TCG)[1]에서 표준화를 진행하고 있다. 이미 많은 PC, 노트북 등에 TPM 하드웨어 및 관련 소프트웨어 기술들이 장착되어 출시되고 있다.

2.2 범용가입자식별모듈(USIM)

USIM(Universal Subscriber Identity Module)은 이동통신기기에서의 가입자 인증용 어플리케이

 Copyright ⓒ 2014 SERSC

션으로 통신용 스마트카드인 UICC(Universal Integrated Circuit Card)에 탑재되어 구동된다. UICC에는 USIM 어플리케이션 이외에도 자바를 이용한 뱅킹, 증권, 신용카드, 전자화폐 등의 다양한 응용서비스를 탑재할 수 있다.

2.3 근거리무선통신(NFC)

근거리무선통신(Near Field Communication, NFC)[4-6] 기술은 13.56MHz 대역의 비접촉식 무선통신 기술로 10cm 이내의 아주 가까운 거리에서 기기간 데이터를 전송하는 기술이다. NFC 기술은 기존의 비접촉식 스마트카드 기술(ISO/IEC 14443 Proximity-card 표준)을 기반으로 개발되었으나 단순 스마트카드 기능 뿐 아니라 양방향 통신을 통해 전자태그의 정보를 읽어오거나 반대로 정보를 입력할 수 있는 Read/Write 기능과 단말간 통신을 위한 P2P 기능까지 제공한다. 신용카드, 신분증 등을 대체할 수도 있으며, 노트북의 사용자 인증, 모바일 티켓, 쿠폰 등 다양한 분야에서 활용될 수 있는 성장 잠재력이 큰 기술이다.

2.4 USB 보안토큰

보안토큰은 스마트카드 기술을 이용하여 물리적 보안기능과 함께 키생성, 암호화, 전자서명 등 암호연산기능을 토큰 내부에서 처리되도록 구현한 하드웨어 기기를 총칭한다. USB 보안토큰은 편리한 USB 형태의 인터페이스를 갖춘 보안토큰으로 사용자 인증 디바이스로 사용된다. 우리나라에서는 해킹 등으로부터 공인인증서 유출을 방지하는 기능을 가진 안전성이 강화된 휴대용 공인인증서 저장매체로 이용되고 있다. TPM이 컴퓨터제조사에 의존하여 운영되고 USIM이 통신회사에 의존하여 운영되는데 반해 USB 보안토큰은 독립적으로 이용될 수 있다는 장점이 있다.

이러한 하드웨어 보안장치들은 암호키의 안전한 저장소로서의 역할뿐만 아니라 RSA기반의 키생성, 암호화, 전자서명, 해쉬, 난수생성 등의 기본 보안기능들을 가지고 있어서 비밀키의 외부 누출이 없이 암호화, 전자서명 등의 보안기능을 하드웨어 장치 내부에서 안전하게 수행할 수 있도록 하는 환경을 제공한다.

그러나 각기 다른 표준화 단체에서 추진하고 있는 이런 기술들은 각각의 기기에서의 키관리는 고려하지만 한 사용자가 여러 개의 서로 다른 종류의 컴퓨팅기기들을 사용하게 되는 유비쿼터스 환경에서 편리하게 사용할 수 있는 통합된 키관리 방식은 제시되지 않고 있다.

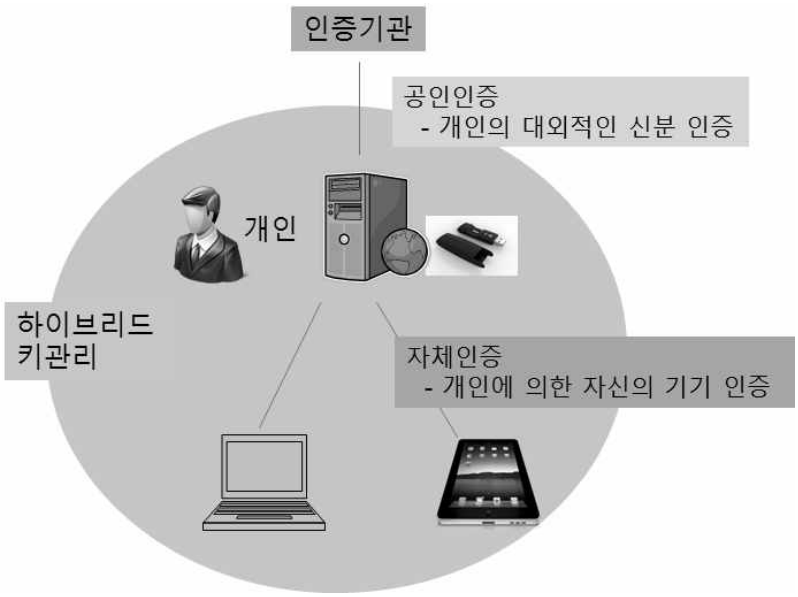
3. 하이브리드 키관리 시스템

3.1 시스템 개요

Copyright ⓒ 2014 SERSC

제안된 하이브리드 키관리 시스템은 인증기관으로부터 발급받은 하나의 인증키를 가지고 있다고 가정했을 때 이것에 기반하여 개인이 소유한 컴퓨팅기기(하드웨어보안모듈) 내에서 생성한 안전한 암호키에 대해 자체인증 방식으로 인증을 확장하여 개인이 새로운 인증키로 사용할 수 있도록 하는 방식이다.

[그림 1]에 도시한 바와 같이 개인은 하나의 키관리서버와 복수개의 컴퓨팅기기들을 소유하고 있는 경우를 고려한다. 외부에 존재하는 신뢰기관인 인증기관은 개인의 신분을 확인하고 인증서를 발급하는 역할을 한다. 키관리서버는 개인이 소유하고 있는 시스템으로 인증서의 안전한 관리를 위하여 하드웨어보안모듈을 장착하고 있다. 개인은 키관리서버를 이용하여 하드웨어보안모듈 내에서 안전한 키쌍을 생성하고 이에 대해 인증기관으로부터 인증서를 발급받는다. 또한 자신이 소유한 하드웨어보안모듈을 장착한 컴퓨팅기기들에서 안전한 기기키를 생성하고 이에 대해 키관리서버를 이용하여 확장인증서명을 발행한다. 확장인증서명이 발행되면 기기키는 확장인증키가 되고 개인이 사용할 수 있는 또 다른 인증키가 된다.



[그림 1] 하이브리드 키관리 시스템 개요

[Fig 1] Overview of hybrid key management system

본 논문에서 사용하는 용어들을 정리해보자.

- 인증키(certified key)란 인증기관이 발행하는 인증서(certificate)를 이용하여 사용자의 장기 신분을 인증해주기 위한 키로 <인증비밀키, 인증공개키>의 쌍으로 이루어진다. 인증서는 인증

Copyright ⓒ 2014 SERSC

키의 유효성과 사용자의 소유를 보증하기 위해 인증기관이 발행하는 문서로서 기존의 X.509 표준[9]에 따른다.

- 개인 소유의 컴퓨팅기기(또는 하드웨어보안모듈) 내에서 사용하는 암호키를 기기키라고 한다. 확장인증서명(extended certification signature)이란 기기키가 특정 사용자의 소유라는 것을 보증하기 위해 사용자 스스로 인증키를 이용하여 발행하는 서명이다. 이것이 발행되면 기기키는 확장인증키(extended certified key)로 인정받는다. 확장인증키는 <확장인증비밀키, 확장인증공개키>의 쌍으로 이루어진다.
- 키관리서버란 개인 소유의 컴퓨터 중에서 인증키를 이용하여 소유 기기들에게 확장인증서명을 발행하는 역할을 하는 컴퓨터를 말한다. 일반컴퓨팅기기는 확장인증키를 장착하고 타인들과의 일상적 보안통신에 이용하는 컴퓨터를 말한다.
- 하드웨어보안모듈은 컴퓨팅기기에 내장된 TPM, 이동통신기기에 내장된 USIM, NFC 칩, 또는 USB 보안모듈 등을 총칭하는 용어이며 사용자의 키관리서버, 컴퓨팅 기기의 상황에 따라 다른 환경을 가질 수 있다. 사용자의 인증비밀키, 확장인증비밀키는 하드웨어보안모듈 내부에서 생성되고 이용되며 외부로 복사해낼 수 없다.

3.2 키관리 시스템의 보안요구사항

개인이 복수의 컴퓨팅기기들을 사용하는 유비쿼터스 환경에서 사용자가 하나의 인증키를 기반으로 자신의 소유기기들에서 사용할 암호키들을 스스로 관리하는 하이브리드 키관리 시스템은 다음과 같은 기능을 가져야 한다.

- 자체관리 – 개인이 외부기관에 의존하지 않고 자신의 소유기기들에 대해 직접 키관리(생성, 폐기) 및 인증을 할 수 있어야 한다.
- 공개적 이용 – 개인이 직접 관리하는 확장인증키들은 개인이 생성하고 인증하는 키이지만 개인의 소유임을 남들에게 인정받고 부인방지 기능을 제공할 수 있어야 한다. 이런 경우 타인과의 공개적인 보안통신에 이용될 수 있다.
- 안전한 키관리 – 개인이 관리하는 확장인증키들은 공격자에 의해 불법적으로 위조되거나 복사될 수 없어야 한다.

3.3 제안 키관리 시스템의 프로토콜

제안된 키관리시스템의 세부 프로토콜을 인증서 발급, 확장인증서명 발행, 확장인증키의 활용으로 나누어 설명한다.

3.3.1 인증서 발급 (인증기관->키관리서버)

Copyright ⓒ 2014 SERSC

개인은 인증기관에게 인증키 발급을 요청하고 인증기관의 요구절차에 따라 인증서를 발급받는다. 인증키의 안전한 관리를 위하여 사용자는 하드웨어보안모듈이 장착된 키관리서버를 이용하여 <인증비밀키, 인증공개키>쌍을 생성하고 인증기관에게 인증공개키를 제출하고 인증서 발급신청을 한다. 인증서가 발급된 인증비밀키는 하드웨어보안모듈의 내부에 저장되고 외부로 누출되지 않는다.

3.3.2 확장인증서명 발행 (키관리서버->소유기기)

사용자는 하드웨어보안모듈이 장착된 소유기기에서 안전한 키쌍을 생성한다. 생성된 공개키에 대해 사용자는 인증키가 장착된 키관리서버를 이용하여 확장인증서명을 발행하고 소유기기에 전달, 저장한다. 확장인증서명이 발행되면 기기키는 사용자의 소유임이 확인된 확장인증키가 된다. 확장인증서명의 상세한 양식은 뒤에서 설명한다.

3.3.3 확장인증키의 활용

사용자는 확장인증키를 장착한 소유기기를 이용하여 타인과 암호화, 전자서명 등 보안통신을 수행할 수 있다. 정당한 사용자만이 소유기기에 접근하고 확장인증비밀키를 사용할 수 있도록 소유기기에 대한 적절한 수준의 접근제어가 제공되어야 한다. 접근제어 방식으로는 비밀번호, 생체인식 등 현재 사용 가능한 다양한 방식이 이용될 수 있다.

사용자(서명자)가 문서에 대해 확장인증비밀키로 서명하는 경우 사용자는 문서에 대한 서명을 하드웨어보안모듈에 요청하고 하드웨어보안모듈은 접근제어를 통해 정당한 사용자임을 확인하고 서명을 생성하여 출력한다. 사용자는 이렇게 생성된 서명문을 인증서와 확장인증서명과 함께 수신자(검증자)에게 제시한다. 서명의 검증자는 다음의 세가지를 함께 확인한다.

1) 인증서 검증을 통해 사용자의 신분을 확인한다.
2) 확장인증서명 검증을 통해 문서의 서명에 사용된 확장인증키가 사용자의 소유임을 확인한다.
3) 서명검증을 통해 확장인증키로 생성된 서명문의 유효성을 확인한다.

사용자(송신자)가 타인에게 암호문을 전달하는 경우 송신자는 수신자의 인증서와 확장인증서명의 유효성을 모두 확인하고 암호문을 전달해야 한다. 암호문을 생성하는 경우에는 상대방의 공개키를 이용하므로 하드웨어보안모듈에서 암호연산을 수행할 필요가 없고 컴퓨터의 본체에서 수행할 수 있다. 송신자는 수신자의 편의성을 고려하여 다음 두가지 방식의 암호화를 함께 제공할 수 있다.

1) 확장인증공개키를 이용한 암호화
2) 인증공개키를 이용한 암호화

이 경우 수신자는 컴퓨팅기기의 하드웨어보안모듈에 저장된 확장인증비밀키를 이용하여 복호화하거나 이것이 어려울 경우에는 키관리서버에 보관된 인증비밀키를 이용하여 복호화를 수행할 수

 Copyright ⓒ 2014 SERSC

도 있다.

3.4 확장인증서명의 양식

이러한 하이브리드 키관리 체계에서 확장인증서명이 수행하는 역할은 인증서와 확장인증키 사이의 위조할 수 없는 결합을 제공하는 것이다. 사용자 스스로 생성하는 이러한 결합이 제공된다면 확장인증서명은 사용자 자신이 인증서로 서명한 문서이므로 확장인증키가 사용자의 신원을 나타내는 또 다른 키라고 해석할 수 있다.

X.509 인증서는 공공의 네트워크에서 타인과의 상호 신분 인증에 사용되며 여기에는 인증기관이 개인에게 부여하는 속성을 제한하기 위해 유효기간, 키이용목적, 확장필드 등의 복잡한 필드들을 가지고 있다. 그러나 확장인증서명의 모델에서는 인증키나 확장인증키 모두 동일한 사용자가 사용하는 것이므로 사용자 내부의 자체인증확장이라고 볼 수 있어서 이러한 복잡한 대외적 기능은 필요하지 않다. 예를 들면 사용자의 자체인증확장에 있어서 유효기간을 제한할 필요가 없다. 이러한 결합기능을 기존의 인증서보다 간단한 형식으로 제공하기 위해서 확장인증서명은 다음과 같은 축소된 형식의 필드들로 구성될 필요가 있다.

[표 1] 확장인증서명의 양식
[Fig 1] Format of extended certification signature

사용자명	확장인증키를 사용하는 사용자의 이름을 나타내며 인증서와 확장인증서명의 결합을 제공하기 위한 핵심 정보이다. 인증서에 표시된 사용자명과 동일해야 유효하다고 판정한다.
인증서 정보	확장인증서명을 발행하는데 사용된 사용자 인증서의 정보를 나타내며 확장인증서명은 이 인증서의 공개키로 검증 가능해야 한다. 사용자의 인증서가 항상 접근 가능한 형태로 제공되는 경우 인증서 정보 필드에는 인증서의 일련번호, 해쉬값 등 축약된 정보를 넣을 수 있다.
기기명	확장인증키를 사용하는 기기의 명칭을 나타내며 사용자가 스스로 구분하기 위한 용도로 활용한다.
확장인증공개키	기기에서 사용할 암호키의 공개키 정보를 나타낸다.
타임스탬프	확장인증서명의 발행 시간을 나타낸다.
서명	위의 모든 필드들을 인증비밀키로 서명한 것이며 인증서에 포함된 인증공개키로 검증 가능해야 한다. 이것은 키관리서버에서 생성된다.

위와 같이 생성된 확장인증서명은 다음과 같이 해석될 수 있다. “인증서에 의해 신분을 확인할 수 있는 사용자가 자신이 활용할 목적으로 안전하게 생성된 키쌍의 공개키에 대해 1) 자신의 소유임을 확인하고, 2) 자신이 안전하게 관리하고 있음을 보증하며, 3) 오용시 책임질 것을 약속하는 의미로 서명을 작성한다.”

Copyright ⓒ 2014 SERSC

확장인증서명에는 확장인증키의 유효기간, 용도, 등이 포함되어 있지 않지만 확장인증키는 사용자의 인증서와 위조할 수 없는 형식으로 결합되어 있으므로 인증서에 포함된 정보를 그대로 준용할 수 있다. 즉, 인증서의 유효성이 보증된 기간 동안에만 확장인증키의 유효성도 보장되며 인증서가 무효화되면 해당 인증서로 발행한 확장인증키도 모두 무효화된다. 그러므로 확장인증키를 사용하는 순간에 다른 사용자는 해당 사용자의 인증서의 유효성을 검증해야 한다.

3.5 확장인증키의 폐기 및 삭제

확장인증키는 사용자가 직접 생성하는 것이고 언제든지 다시 생성할 수 있으므로 쉽게 삭제 가능하다. 그러므로 다음과 같은 상황에서 확장인증키를 쉽게 폐기할 수 있다.

1) 사용자가 소유기기를 타인에게 양도시에는 하드웨어보안모듈에 내장된 확장인증키비밀키를 삭제 후 양도하면 된다.
2) 기기 분실시의 안전성을 위한 대책으로 정해진 횟수 이상 시스템 접근이 실패할 경우 내장된 확장인증키를 자동 삭제하도록 운영할 수 있다. 기기 습득자는 시스템 접근제어를 통과하지 못하는 경우 확장인증키가 자동 삭제되고 사용자의 이름으로 기기를 사용할 수 없다. 사용자가 기기를 분실한 경우 확장인증비밀키를 원격으로 삭제할 수 있도록 기능을 넣을 수 있다.
3) 사용자가 기기에의 접근암호를 잃어버려 사용하지 못하게 되었을 경우 키쌍을 다시 생성하고 확장인증서명을 다시 발행하여 사용할 수 있다.
4) 확장인증키의 유효성을 중단시키기 위해 사용자는 인증서를 폐기하고 재발급 받을 수도 있다. 인증서가 취소된 경우 이미 사용하고 있는 모든 확장인증키와 확장인증서명은 유효성을 상실하게 되며 새롭게 생성되어야 한다.

4. 제안 방식의 특성 분석

4.1 제안 방식의 특징

이 논문에서 제안된 하이브리드 키관리 방식은 다음의 보안요구사항을 만족시킬 수 있다.

- 자체관리 - 위에서 제시한 바와 같이 개인은 외부기관에 의존하지 않고 자신의 소유기기들에 대해 직접 키관리(생성, 폐기) 및 인증을 할 수 있다.
- 공개적 이용 - 개인이 직접 관리하는 확장인증키들은 개인이 생성하고 인증하는 키이지만 인증키로 직접 서명한 확장인증서명과 함께 사용되므로 남들에게 유효성을 인정받을 수 있고 부인방지 기능을 제공할 수 있다.
- 안전한 키관리 - 개인이 관리하는 확장인증키비밀키는 하드웨어보안모듈 내부에서 생성되고 운영되며 외부로 꺼낼 수 없으므로 공격자에 의해 불법적으로 위조되거나 복사될 수 없

 Copyright ⓒ 2014 SERSC

다. 기기에 대한 접근제어 메커니즘을 통해 공격자의 접근을 차단함으로써 공격자가 사용자의 이름으로 이용하는 것을 방지할 수 있다.

제안된 하이브리드 키관리 방식은 다음과 같은 특징을 가지고 있다.

- 운영의 편의성 - 제안된 키관리 방식을 이용하면 새로운 기기를 도입할 때마다 사용자 스스로 안전한 암호키를 생성하고 확장인증서명을 발행하여 새로운 인증키로 이용할 수 있어서 기존의 기기별 독립적인 키관리 방식보다 운영의 편의성을 크게 향상시켰다. 그러므로 개인은 하나의 인증키만 안전하게 잘 관리하면 개인소유의 모든 기기들에서 인증이 자체확장된 키들을 배포하고 활용할 수 있다.
- 키삭제 가능 - 확장인증키는 사용자가 직접 생성하는 것이므로 언제든지 필요시 생성할 수 있고 기존의 키를 삭제하는 것도 가능하다. 그러므로 기기의 분실시, 사용자가 기기 접근 암호를 분실시 키를 삭제하고 다시 생성할 수 있다.
- 확장인증키의 정적 특성 - 확장인증서명은 유효기간, 폐기 메커니즘 등의 가변적인 정보가 없이 정적인 특성을 가져서 한번만 서명검증을 하면 인증서의 유효기간까지 추가적인 서명검증 없이 사용할 수 있다.
- 표준 중립성 - 제안된 키관리 방식은 하드웨어보안모듈에서 생성된 키쌍의 공개키에 대해 사용자가 확장인증서명을 발행하여 사용하는 방식이다. 그러므로 이러한 키관리 방식은 기존의 TPM, USIM, 보안토큰, NFC 등의 하드웨어보안모듈 관련 표준들을 수정하지 않고 그대로 사용할 수 있으며 운영체제 또는 응용프로그램 수준에서 확장인증서명을 발행하고 이용하는 기능만 추가하면 된다.
- 인증서의 안전한 관리 - 제안된 키관리 체계에서 인증서는 확장인증서명을 발행하는 용도에만 사용하고 타인과의 보안통신에는 직접 사용하지 않도록 할 수 있다. 그러므로 키관리서버는 인증서 발급, 확장인증서명 발행시에만 사용하고 인터넷에의 접속을 끊거나 전원을 끌 수 있다. 그러므로 인증서의 대외적 노출이 최소화되고 인증비밀키가 저장된 키관리서버에 대한 공격을 최소화하여 인증서를 더욱 안전하게 관리할 수 있게 된다.

4.2 안전성 분석

제안된 하이브리드 키관리 방식은 키관리의 안전성을 위하여 하드웨어보안모듈을 사용하는 것을 가정하고 있다. 하드웨어보안모듈의 하드웨어적 안전성을 가정할 때 그 내부에서 생성되는 키쌍의 비밀키는 외부로 빼낼 수 없으며 전자서명 등 비밀키를 필요로 하는 연산은 하드웨어보안모듈 내부에서 실행되도록 운영된다.

확장인증서명은 기기에 내장된 확장인증키가 사용자의 인증서와 강하게 결합되어 있다는 것을 보여주는 문서로서 인증서로 서명된 문서인데 키관리서버에 있는 하드웨어보안모듈에서 생성된다.

Copyright ⓒ 2014 SERSC

키관리서버에의 접근암호를 모르는 타인은 확장인증서명을 위조할 수 없다. 더구나 키관리서버는 오프라인 상태로 운영되거나 평상시 전원을 꺼놓을 수 있어서 온라인 공격자에게 더욱 안전하게 관리될 수 있다.

기기 및 하드웨어보안모듈의 이용에는 정당한 소유자만이 이용할 수 있도록 적절한 수준의 접근제어 메커니즘이 적용되어야 한다. 안전한 접근제어가 있다고 가정할 경우 기기를 습득한 타인은 사용자의 명의로 기기를 이용할 수 없다.

4.3 성능 분석

사용자가 1개의 키관리센터와 n개의 컴퓨팅기기를 소유하고 이용한다고 가정하자. 먼저 n개의 컴퓨팅기기별로 서로 다른 인증서를 발급받아 사용하는 경우와 비교해보자. 사용자는 n개의 인증서를 관리해야 하며 인증서는 발급, 폐기, 재발급의 문제를 야기하는데 이것을 사용자가 직접 관리해야 한다. 새로운 기기를 구입할 때마다 인증기관과 인증서 발급 프로세스를 수행해야 하며 기기를 분실하게 되면 또한 인증서의 폐기, 재발급 프로세스를 수행해야 하는데 이것은 일반 사용자에게 매우 부담스러운 일이다.

이 논문에서 제안된 하이브리드 키관리 방식을 이용하면 사용자의 키관리가 매우 간편해진다. 키관리센터에는 사용자의 인증서를 내장하고 있으며 각각의 컴퓨팅기기에는 사용자가 생성한 확장인증키를 내장하고 있다. X.509 형식의 인증서는 인증기관에 의한 인증서 폐기의 가능성이 있으므로 매번 사용시마다 인증서의 유효성을 온라인 검증해야 한다. 그러나 제안된 확장인증서명은 사용자가 생성한 고정된 문서이므로 유효성 검증을 최초 한번만 하면 된다. 그러므로 서명의 검증자 입장에서는 서명자 인증서의 유효성만 확인하면 각각의 확장인증키의 유효성을 즉시 확인할 수 있게 된다. 사용자 입장에서는 하나의 인증키만 안전하게 관리하면 자신 소유의 n개의 기기들에서 인증키를 자체 생성하고 이용할 수 있으므로 키관리의 편의성을 크게 높인 것이 된다. 계산량 측면에서 비교해보면 사용자의 인증서에 대해서는 항상 유효성을 확인해야 하기 때문에 두가지 방식 모두 인증서 검증이 필요하다.

5. 결론

이 논문에서는 사용자가 복수개의 컴퓨팅기기들을 사용하는 유비쿼터스 환경에서 하나의 인증키에 기반하여 복수의 확장된 인증키들을 생성하고 사용하는 방식을 제시하였다. 이 방식은 TPM, USIM, 보안토큰, NFC 등 하드웨어 방식의 보안모듈을 장착하여 사용하는 컴퓨터에서 사용자의 인증키들을 매우 편리하게 관리할 수 있는 방식이다. 제안된 방식은 하드웨어보안모듈에 키를 외부로부터 입력하거나 외부로 출력하지 않고 하드웨어보안모듈 내부에서 생성되고 안전하게 보호되고 있는 키에 대하여 확장인증서명을 통해 사용자가 인증을 자체확장하는 방식이다.

 Copyright ⓒ 2014 SERSC

현재까지는 이러한 새로운 인증 및 키관리 방식을 사용할 수 있는 기술적, 제도적 뒷받침이 미비한 상황이지만 유비쿼터스 환경의 확대와 함께 개인에 의한 복수 기기에서의 키관리의 어려움을 고려할 때 제시한 것과 같은 개인화된 키관리 방식의 도입을 적극 검토할 필요가 있다.

Copyright ⓒ 2014 SERSC

References

[1] http://www.trustedcomputinggroup.org/, Aug. 2. (2014)

[2] J. S. Park, T. N. Cho, J. H. Han, and S. I. Jun, Trusted Computing Technology and TCG Standard Trend, Electronics and Telecommunications Trends, (2008), Vol. 23 No. 4, pp. 48-59.

[3] Siani Pearson, et al., Editor, Trusted Computing Platforms, Prentice Hall PTR (2003)

[4] H. J. Kim, T. K. Kwon, NFC Technology Trends and Security Issues, Information and Communications Magazine (Information and Communications). (2012), Vol. 29 No. 8, pp. 57-64.

[5] http://www.nfc-forum.org/, Aug. 20 (2014)

[6] Jonghyun Baek, HeungYoul Youm, NFC-based mobile service security risk and measure, Review of KIISC. (2013), Vol. 23 No. 2, pp. 55-65.

[7] M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures: Delegation of the power to sign messages, In IEICE Trans. Fundamentals. (1996), Vol. E79-A, No. 9, Sep., pp. 1338-1353.

[8] Byoungcheon Lee, Heesun Kim, and Kwangjo Kim, Strong Proxy Signature and its Applications, The 18th Symposium on Cryptography and Information Security, (2001), Jan. 23-26, 11B-1, pp. 603-608; Osio, Japan.

[9] http://www.ietf.org/rfc/rfc2459, Aug. 20 (2014)

Authors

이병천 (Byoungcheon Lee)

1986년 2월 : 서울대학교 물리학과 학사
1988년 2월 : 서울대학교 물리학과 석사
2002년 2월 : KAIST 정보보호 박사
2002년 3월 ~ 현재 : 중부대학교 정보보호학과 교수
관심분야 : 암호 프로토콜, 네트워크 보안, 인증

Copyright ⓒ 2014 SERSC