하드웨어 보안모듈을 장착한 컴퓨팅기기에서의 유비쿼터스 키관리 방안

이병천*

*중부대학교 정보보호학과

Ubiquitous Key Management in Computers Equipped with Hardware Security Module

Byoungcheon Lee*

*Department of Information Security, Joongbu University.

요 약

개인이 여러 대의 컴퓨팅 기기들을 사용하는 유비쿼터스 환경에서는 개별 기기에서의 키관리뿐만 아니라 사용자가 자신이 소유한 복수의 컴퓨팅 기기들에서 안전하고도 편리하게 키를 체계적으로 관리할 수 있어야 한다. 요즘 발매되는 최신형 컴퓨터들은 하드웨어 기반의 보안칩인 TPM[2]이 장착된 형태로 출시되고 있으나 이것을 적극 활용하는 것은 아직 활성화되지 않고 있다. 이 논문에서는 하드웨어 보안모듈을 장착한 컴퓨팅기기에서의 키관리 방안으로서 개인이 소유한 하나의 인증키를 기반으로 복수의 소유 기기들에서 안전하게 생성되는 키들에게 인증을 자체 확장하여 이용할 수 있는 효율적인 방안에 대해 제안하고자 한다.

I. 서론

개인이 복수의 컴퓨팅 기기들을 사용하게 되는 유비쿼터스 환경에서는 키관리의 개인화가 필요하다. 개인이 인증키를 사용할 수 있기 위해서는 인증기관으로부터 인증서를 발급받아 사용하는 것이 일반적인 접근방법인데 개인이 복수의 기기들을 사용하는 경우 기기별 인증을 어떤 방법으로 제공할지가 관건이다.

첫째, 하나의 인증키를 여러 기기들에 복사하여 사용하고자 하는 경우 비밀키가 기기 외부로 복사되고 통신을 통해 전달되므로 공격자에게 탈취될 수 있는 위험이 있다. 이런 경우 하나의 기기에서라도 비밀키가 공격자에게 탈취된다면 다른 모든 기기에서도 그 키를 사용할 수 없게 되는 문제가 있다. 만일 비밀키를 외부로 복사해낼 수 없는 하드웨어 보안장치에서 생성된 키쌍에 대해 인증서를 발급받는 경우 비밀키를 하드웨어 외부로 복사할 수 없다는 근본적인 문제점이 있다.

둘째, 각 기기별로 별도의 인증을 받아서 사용하는 경우 개인 사용자가 인증기관과의 인증서 발급 프로세스에 여러 번 관여해야 하며 인증기관에게 자신의 신분을 여러 번 확인해야 하는 불편함이 있다. 또한 발급된 여러 개의 키와 기기들을 개별적으로 안전하게 관리해야 하는데 개인에게 이것은 매우 어려운 문제이다.

이러한 문제를 해결하기 위해서는 개인이 소유한 복수의 컴퓨팅 기기에서의 편리하고도 안전한 키관리를 위한 체계적인 해결책이 제시되어야 한다.

한편 요즘 발매되는 최신형 컴퓨터들은 하드웨어 기반의 보안칩인 TPM(Trusted Platform Module)[2]이 메인보드에 장착된 형태로 출시되고 있다. 하드웨어보안모듈이라 불리는 HSM (Hardware Security Module)[4]을 컴퓨터에 연결하여 보안기능을 활용하기도 한다. 스마트폰, 태블릿컴퓨터 등의 이동통신 단말기들도 범용 가입자식별모듈인 USIM(Universal Subscriber

Identity Module) 등의 보안기능을 가진 하드웨어 장치를 기본 장착하고 있다. 이러한 보안칩들은 암호키의 안전한 저장소로서의 역할뿐만 아니라 RSA기반의 키생성, 암호화, 전자서명, 해쉬함수, 난수생성 등의 기본 보안기능들을 가지고 있어서 비밀키의 외부 누출이 없이 암호화, 전자서명 등의 보안기능을 하드웨어 칩 안에서 수행할 수 있도록 하는 환경을 제공한다.

현재의 공인인증 기반 전자상거래 시스템에 대해 많은 비판이 존재하는데 이것은 액티브엑스 형태의 비표준 부가프로그램을 브라우저에 설치해야 한다는 점과 컴퓨터 내부에 비밀키를 안전하게 보관하고 사용하기 어려워 각종 해킹 공격에 대응하기 어렵다는 점 때문이다. 이러한 하드웨어 보안칩이 적용된 컴퓨터는 비밀키의 안전한 보관과 사용이 가능하고 부가프로그램 설치가 필요없어서 공인인증체계의 고도화에 큰 도움이 될 것으로 예상된다. 그러나 이러한 하드웨어 보안칩의 기능을 적극 활용하는 것은 아직 널리 활성화되지 못하고 있다.

이 논문에서는 하드웨어 보안모듈을 장착한 컴퓨터의 우수한 키관리 기능을 적극 활용하는 방법으로서, 개인이 가지고 있는 하나의 인증키를 기반으로 개인이 소유하고 있는 기기의 하드웨어 보안모듈에서 안전하게 생성한 기기키에 대해 인증서명을 생성함으로써 인증을 복수의 키들에게 자체 확장하여 사용하는 방안을 제시한다.

II. 하드웨어 보안모듈

현재의 컴퓨팅 환경과 인터넷 통신 환경은 다양한 해킹공격에 취약성을 가지고 있어서 컴퓨터가 당초 의도된 대로 동작하고 있다는 것을 보증하기가 어려운 환경이다. 표준 운영체제에서 동작하는 소프트웨어만으로는 이러한 공격에 대응하기 어려워 별도의 운영체제와 제한된 통신기능을 가지며 Tamper proof 기능을 가지는 하드웨어 보안모듈을 통해 보안기능을 구현하려는 노력이 이루어지고 있다. 현재의 컴퓨팅 환경에서는 다음과 같은 보안모듈들이 사용가능하다.

■ HSM(하드웨어보안모듈)[4] - PCI, SCSI, 이더넷 등의 인터페이스를 통해 서버와 연결되어 높은 수준의 키관리 기능을 제공하는 하드웨어 암호장비이다.

■ 보안토큰 - USB 포트에 연결하는 형태의 하드웨어 보안장치이다.

■ USIM(가입자인증식별모듈) - 휴대전화용 가입자 식별 카드로서 스마트카드와 같은 보안기능을 탑재하고 있다.

■ TPM(신뢰플랫폼 모듈)[2,3] - 컴퓨터 메인보드 내에 설치된 하드웨어 보안칩을 말하며 신뢰컴퓨팅그룹(TCG)[1]에서 표준화를 진행하고 있다.

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

그러나 각기 다른 표준화 단체에서 추진하고 있는 이런 기술들은 각각의 기기에서의 키관리는 고려하지만 여러 개의 서로 다른 종류의 컴퓨팅기기들을 사용하게 되는 사용자 입장에서 편리하게 사용할 수 있는 통합화된 키관리는 고려되지 않고 있다. 가능하다면 각 기기별 표준을 지키면서도 운영체제 또는 응용프로그램 수준에서 인증을 확산하여 개인이 직접 키를 관리하는 방법이 필요하다.

III. 제안 키관리 방식

3.1 용어

여기에서는 본 논문에서 사용하는 용어들을 정리하고자 한다.

o 인증키 - 신뢰하는 인증기관이 발행하는 인증서를 통해 사용자의 장기 신분을 인증해주는 키.

o 기기키 - 각 컴퓨팅 기기들의 하드웨어 내에서 생성되고 저장되어 안전하게 사용할 수

있는 키.

o 인증서 - 인증키의 유효성을 보증하기 위해 인증기관이 발행하는 전자문서.

o 기기인증서명 - 기기키의 유효성을 보증하기 위해 사용자 스스로 자신의 인증키를 이용하여 발행하는 서명.

o 키관리서버 - 인증키를 이용하여 소유 기기들의 기기키에 대한 기기인증서명을 발행하는 역할을 하는 컴퓨터.

o 일반컴퓨터 - 기기키를 장착하고 있으며 사용자가 일상적 용도에 이용하는 컴퓨터.

3.2 키관리 방식

1) 인증서 발급

사용자는 키관리서버에 내장된 TPM에서 키쌍을 생성하고 인증기관에게 인증서 발급을 요청하고 인증서를 발급받는다. 인증된 비밀키는 TPM 내부에 저장된다.

2) 기기인증서명 발행

사용자는 일반컴퓨팅기기에 내장된 TPM에서 기기키 쌍을 생성하고 그 공개키에 대하여 키관리서버에서 인증비밀키로 서명하여 기기인증서명을 발행한다. 기기인증서명은 공개될 수 있는 문서로서 기기 내에 저장하고 통신을 통해 타인에게 전달할 수 있다.

3) 기기키 이용

사용자는 기기키가 장착된 일반컴퓨터를 이용하여 일상적 보안통신에 활용한다. 타인에게 기기키의 인증성을 제시하기 위해서는 자신의 인증서와 함께 기기인증서명을 함께 첨부한다.

3.3 기기인증서명의 양식

암호키를 인증하기 위해 사용하는 일반적인 방식은 PKI 기반의 인증서를 이용하는 것인데 이것은 개인의 대외적인 신분을 확인하기 위한 용도로 사용되기 때문에 매우 복잡한 체계를 가지고 있다. 개인이 이미 소유하고 있는 인증을 확장하여 자신이 소유한 기기들에게 인증키를 발행하는 용도에는 별도의 간략화된 서명형식을 정의하고 활용하는 것이 좋을 것이다. 본 논문에서 제안하는 기기인증서명에는 다음과 같은 정보들이 포함될 필요가 있다.

1) 사용자명 - 기기의 사용자를 나타내며 인증서에 표시된 사용자명과 동일해야 한다.

2) 인증공개키 - 인증서에 포함된 공개키로 기기인증서명을 검증하는데 이용된다.

3) 인증서 해쉬값 - 기기인증서명과 인증서와의 분리할 수 없는 링크를 제공하기 위하여 인증서의 해쉬값을 포함한다.

4) 기기명 - 기기의 명칭

5) 기기공개키 - 기기의 보안모듈에서 생성한 키쌍의 공개키

6) 타임스탬프 - 기기인증서명의 생성시간

위와 같은 정보에 사용자의 인증비밀키로 서명하여 기기인증서명을 발행한다.

3.4 기기키의 사용

TPM이 장착된 컴퓨터를 이용하여 메시지에 대해 서명하고자 하는 경우 (메시지, 인증서, 기기인증서명)을 포함한 문서에 기기비밀키를 이용하여 서명한다. 검증시에는 1) 인증서 검증, 2) 기기인증서명 검증, 3) 서명 검증의 단계를 거쳐 세가지 모두 유효한 경우에 사용자의 유효한 서명으로 인정한다.

3.5 기기키의 취소 방법

TPM이 장착된 컴퓨터에서 기기비밀키를 추출하는 것은 어렵지만 기기를 분실하거나 타인에게 양도하는 경우 기기키의 유효성을 폐지해야 한다. 이 경우 기기키를 취소할 수 있는 방법은 다음과 같은 방식이 있을 수 있다.

1) TPM의 기기키를 삭제하고 타인에게 양도한다.

2) 기기를 분실한 경우 기기키취소목록, 또는

유효한 기기목록을 서명, 발행하여 함께 사용하도록 할 수 있다.

3) 기존의 인증서를 취소하고 새로 발급받는다. 인증서가 취소된 경우 이미 사용하고 있는 모든 기기키와 기기인증서명은 유효성을 상실하며 새롭게 생성되어야 한다.

IV. 제안방식의 특성 분석

1) 기기비밀키는 TPM 내부에 저장되고 서명연산도 TPM 내부에서 수행되므로 기기비밀키는 밖으로 노출되지 않는다. 컴퓨터는 터미널 역할만 수행하고 비밀키를 이용하는 암호연산은 TPM에 의뢰하여 수행하고 결과만 얻게 된다. 기기의 분실시 TPM 이용에 적절한 수준의 접근제어가 설정되어 있다고 가정할 경우 타인이 키를 도용할 수 없다.

2) 개인의 키관리의 편의성이 크게 향상되었다. 개인은 하나의 인증키만 안전하게 잘 관리하면 개인소유의 모든 기기들에 인증이 확장된 키들을 생성하고 활용할 수 있다.

3) 인증서의 유효기간이 지나거나 취소된 경우 각 기기의 키들에 대한 기기인증서명도 유효하지 않게 된다. 이 경우 새롭게 발급된 인증서에 기반하여 기기인증서명을 갱신해야 한다.

4) 제안방식은 기기공개키에 대한 기기인증서명을 발행하여 사용하는 방식으로 이것은 공개될 수 있는 정보이므로 기존의 TPM, USIM, HSM, 보안토큰 등의 하드웨어 보안모듈 관련 표준들을 수정하지 않고 운영체제 또는 응용프로그램 수준에서 체계적인 키관리가 가능하게 된다.

V. 결론

이 논문에서는 TPM, USIM, HSM, 보안토큰 등 하드웨어 방식의 보안모듈을 장착하여 사용하는 컴퓨터에서의 체계적인 인증키 관리 방식을 제안하였다. 사용자가 복수개의 컴퓨팅기기들을 사용하는 유비쿼터스 환경에서 하나의 인증키에 기반하여 복수의 기기키들에 대해서도 인증을 자체적으로 확장하여 사용하는 방식이다. 하드웨어 보안모듈에 키를 외부로부터 입력하거나 외부로 출력하지 않고 하드웨어 보안모듈 내부에서 생성되고 안전하게 보호되고 있는 키에 대하여 외부에서 제공하는 기기인증서명을 통해 인증성을 확대하는 방식이다. 이것은 기존의 하드웨어 보안토큰의 표준들을 수정할 필요 없이 보안토큰 내에서 생성된 키에 대해 사용자 스스로 기기인증서명을 발행하여 사용하는 방식으로 컴퓨터 내에서 운영체제수준 또는 응용프로그램 수준에서 키관리를 수행할 수 있도록 한다. 기기키에 대해 사용자가 인증키로 서명한 기기인증서명을 첨부하므로 타인들도 서명의 유효성을 인정할 수 있게 된다.

[참고문헌]

[1] Trusted Computing Group, http://www.trustedcomputinggroup.org/

[2] 박정숙, 조태남, 한진희, 전성익, Trusted Computing 기술 및 TCG 표준화 동향, 전자통신동향분석 제23권 제4호, pp 48-59, 2008. 8.

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

[4] PCI Security Standards Council, PCI HSM Security Requirements v1.0, 2009.