MTM 기반의 모바일 신뢰 컴퓨팅을 위한 안전한 키 백업 방안에 대한 연구†

강동완*, 전성익**, 이임영*
*순천향대학교 컴퓨터학부, **한국전자통신연구원
e-mail : lupin428@sch.ac.kr

A Study on Key Backup Mechanism for MTM based Mobile Trusted Computing Environment

Dong-Wan Kang*, Sung-Ik Jun**, Im-Yeong Lee*
*Division of Computer Science and Engineering, Soonchunhyang Univ.
**Electronics and Telecommunications Research Institute

요 약

현대의 서비스들은 점차 온라인화 되어 가고 있으며, 특히 무선 통신의 발전은 따라 현대 사회인들에게 다양한 모바일 기기들을 사용하여 여러 서비스를 제공 받을 수 있도록 하였다. 하지만 모바일 단말기의 분실 및 불법적인 복제와 점차 증가하고 있는 모바일 악성코드로 인한 모바일 환경의 보안 위협은 기존의 소프트웨어 보안으로는 감당할 수 없게 되었다. 이에 안전한 모바일 환경을 위해 하드웨어 모듈 기반의 신뢰 컴퓨팅이 제안되었다. 이는 하드웨어 보안 모듈로 하여금 보안 시스템의 중추적인 역할을 하도록 하여 전체 보안 수준을 하드웨어 수준으로 높이는 장점을 가지고 있다. 하지만 이러한 하드웨어 기반의 보안 시스템에서는 사용자의 암호 및 단말기 이동에 따른 적절한 키의 백업과 복구 방안이 필요하다. 본 논문에서는 이러한 MTM 기반의 모바일 신뢰 컴퓨팅에서의 키 백업에 대한 보안 요구사항과 메커니즘에 대한 분석을 제시한다..

1. 서론

모바일 환경의 보안은 기존의 유선 환경보다 훨씬 열약한 환경을 가지고 있다. 무선의 특성으로 통신 트래픽을 쉽게 얻을 수 있으며, 모바일 단말기의 분실 및 물리적인 해킹은 모바일 환경의 주된 보안 위협으로 볼 수 있다. 특히 현재 사용하고 있는 모바일 단말기의 한 종류로써 핸드폰의 경우, 사용자는 자신의 핸드폰에 비밀번호를 걸어 놓지만 이는 사용자의 개인정보를 모른다고 하더라도 일반적인 전사적 공격에 의해 매우 취약하다. 이러한 패스워드 기반의 인증 방법은 사용자가 직접 기억해야 하는 패스워드를 사용해야 하므로 그 패스워드의 암호학적 강도가 높지 않은 것이 사실이다.

따라서 USIM(Universal Subscriber Identity Module)를 사용하여 사용자를 인증하는 방안이 연구되어 이동전화 서비스를 위한 가입자 인증 방안으로 사용되고 있다. USIM 은 사용자를 인증하기 위한 인증정보를 하드웨어적으로 안전하게 저장하기 때문에 사용자는 그것을 자신이 기억하지 않아도 되며 단지 USIM 에 대한 사용자의 소유자 인증을 수행하면 된다. USIM 은 모바일 단말기와 서로 독립적인 사용자 인증을 위한 다른 하드웨어적 보안 요소이기 때문에 USIM 을 사용함으로써 내가 사용하고자 하는 단말기가 정당한 단말기인지 판단할 수 있어야 한다. USIM 은 사용자의 인증정보가 저장되어 있기 때문에 불법적인 단말기나 악의적인 목적을 가진 단말기를 사용하게 될 경우 사용자의 개인 정보가 유출되거나 악용될 우려가 있기 때문에 모바일 단말기에 대한 인증을 위한 보안적인 요소가 필요하다.

핸드폰을 포함한 모바일 단말기를 사용하기 위해서 이루어지는 인증 과정의 패스워드와 서비스를 이용함에 있어서 사용되는 암호키 및 전자서명용 키, 인증서 등의 정보는 매우 중요한 정보이며 저장되는 위치 및 주체에 따라서 관리에 대한 취약점이 존재한다. MTM 을 사용하기 위한 사용자 인증 정보 및, 서비스 이용에 따른 사용자 패스워드는 사용자가 기억하는 정보로써 유사시 복구에 대한 대책이 요구되며, MTM 기반의 관리하에서 관리되고 있는 키 또한 물리적 손

† 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음.
[2006-S-041-03, 차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통 보안 핵심 모듈 개발]

상에 대비한 백업 방안이 필요하다. 본 논문에서는 이러한 MTM 기반의 모바일 신뢰 컴퓨팅 환경에서 키 백업에 대한 보안 요구사항과 관련 기술을 분석하여 각각의 효용성을 분석하고자 한다.

2. 보안 요구 사항

본 장에서는 키 백업 기술에 대한 일반적인 개념과 그 대상에 따라서 제공 되어야 하는 보안 요구사항에 대해서 기술한다.

2.1 키 백업의 개념

키 백업의 개념은 키 관리의 한 부분으로써 정당한 객체가 어떤 특정한 사건을 계기로 하여 정당한 권한을 행사할 수 없을 때 그 권한을 원래대로 돌려놓는 것이다. 암호학에서의 키 백업은 키의 소유자가 키를 분실하거나 혹은 의도하지 않은 손상으로 인해서 정당하게 암호화 된 개체에 접근할 수 없을 때 그 키를 복구하는 것으로 설명될 수 있다. 현대 정보사회에서의 암호 사용이 증가함에 따라 보다 강력한 보안 정책을 사용하게 되고 이에 따른 키 관리의 어려움에 따라 키 복구의 중요성은 나날이 증가하고 있다고 할 수 있다. 따라서 이러한 키 복구의 한 방법으로써 키 백업을 통해 해당 키의 복사본을 다른 안전한 곳에 보관하는 방법으로 키 복구를 지원할 수 있다.

2.2 키 백업에서의 보안 요구사항

백업되는 데이터는 암호화된 키뿐만 아니라 전자서명된 데이터의 유효성을 검증하기 위한 공개된 공개키 인증서 또한 보호해야 할 데이터 이다. 다만 암호화 에 사용된 대칭키 및 개인키는, 공개된 공개키와 비교하여 기밀성이 높게 요구된다. 키 백업의 일반적인 개념에 있어서 보안 요구 사항에 대해 다음의 사항이 적용 될 수 있다.

• 인증 : 백업 데이터를 생성하거나, 백업 데이터에 대한 복원 프로세스는 사전에 정의된 정당한 사용자 및 권한자에 의해서만 이루어 져야 한다. 이를 위해서 백업 시스템은 절차에 따른 객체에 대한 인증을 수행해야 한다.

• 기밀성 : 백업 대상의 정보는 원래 키의 소유나 혹은 정당한 절차에 의해 복호되는 경우를 제외하고 다른 제 3 자에 의해 키의 정보가 노출되어서는 안된다.

• 무결성 : 암호화 되어 백업된 키가 변조나 위조 등으로써 해당 정보가 원래 보관 하고자 했던 키 정보와 비교하여 변경되지 않았다는 것을 증명할 수 있어야 한다.

• 가용성 : 암호키에 대한 백업 프로세스는 언제나 그 동작을 수행할 수 있어야 하며, 어떠한 상황이 오더라도 보관, 혹은 유지하고 있는 정보들에 대해서 정당한 객체가 접근할 수 있도록 해야 한다.

• 안전한 저장소 : 백업되는 데이터는 해당 사용자에 대한 비밀 정보로써 해당 데이터에 대한 파괴 및 삭제, 악의적인 변조등은 백업 시스템을 무력하게 만들 수 있다. 백업 시스템은 이러한 공격에 대해 탐지하는 것뿐만 아니라 적극적인 복구도 가능하도록 설계되어야 한다.

3. 관련 연구

본 장에서는 관련 연구로써 신뢰 컴퓨팅의 기반이 되는 MTM 과 MTM 내부의 안전한 키 유출을 위한 키 이전 방안으로써 Migration 과 Maintenance, 그리고 신뢰 모듈을 사용하는 상용 서비스로써 Microsoft 사의 BitLocker 드라이브 암호 시스템의 키 복구 메커니즘을 분석한다.

3.1 MTM

MTM 은 TCG(Trusted Computing Group)에서 제안한 TPM(Trusted Platform Module)의 모바일 버전이다[2] MTM 은 플랫폼에 임베디드 되어 동작하며 물리적인 공격에 저항성을 가지고 있고, 시스템과 독립적인 개체로써 자신의 연산 과정을 외부에 노출 시키지 않는다. MTM 이 내부의 비휘발성 저장매체에 가지고 있는 SRK(Storage Root Key)는 MTM 에서 사용하는 키들을 보호하기 위한 계층적인 트리 구조의 최상단 루트 키로써 안전한 저장매체를 이루는 핵심적인 키이다. 실제 암호키는 MTM 안에서만 접근이 가능하기 때문에 단말에서 사용되는 암호키의 안전한 관리가 가능하고 외부 저장매체에 대해서 안전한 영역을 보장할 수 있다.

3.2 Migration & Maintenance

TCG 는 임베디드된 특성을 가진 TPM/MTM 을 사용하는데 있어 플랫폼의 변경에 따라서 모듈 내부의 암호키를 모듈 밖으로 빼내어 다른 모듈로 이전시키는 메커니즘을 정의하였다. 이 메커니즘은 Migration 과 Maintenance 로 정의되며, 이를 사용하여 보안 모듈 내부의 암호키를 다른 모듈로 이동시킬 수 있다[3].

TPM 에서 사용되는 키는 모두 속성을 가지고 있으며 그중에 migration 에 관한 속성이 정의되어 있다. 이는 migratable 과 non-migratable 속성 중 한가지를 가지게 된다. Migratable 은 Migration 메커니즘을 사용하여 다른 TPM 으로 이동할 수 있는 키 이며, non-migratable 속성을 가진 키는 Migration 메커니즘으로 이동시킬 수 없고, Maintenance 메커니즘을 통해서만 다른 TPM 으로 이동시킬 수 있는 키 이다.

Migration 과 Maintenance 는 TPM 에서 키를 외부의 다른 TPM 으로 이동시키는 수단으로써 키 백업보다는 플랫폼 이전에 따른 키의 이동으로 제안되었다. 또한 이들 메커니즘은 표준 문서에 그 절차가 기술되어 있지만 실질적인 구현 방안에서는 TPM 제조사에

위임하고 있다. 더욱이 Maintenance 의 경우에는 필수적으로 구현 사항이 아니기 때문에 여타 다른 TPM 제조사들간의 Maintenance 는 상당한 어려움이 예상된다. 언급된 Migration 과 Maintenance 이 외에 TPM 에서의 키 복구 방안은 현재 제안된 형식이 없으며 따라서 TPM 을 사용하는 데에 따른 적절한 키 복구 방안은 지속적으로 연구가 필요하다.

3.3 BitLocker

BitLocker 는 Windows Vista 에서 새롭게 나온 보안 솔루션으로 하드디스크 전체를 암호화 하는 보안 기능을 가지고 있다[1]. 이 BitLocker 는 TPM(Trusted Platform Module)[4]을 사용하여 암호화를 수행하는데 256bit 의 FVEK(Full Volume Encryption Key)로 AES 암호화를 통해 디스크를 보호한다. FVEK 는 TPM 에 의해 보호되며 해당 TPM 에 의해서만 복호될 수 있다. BitLocker 는 FVEK 에 대해 다음과 같이 복구 방법을 제공한다.

- 복구 암호를 통한 복구
- 복구 키를 통한 복구
- AD(Active Directory) 를 사용한 복구

복구 암호를 통한 복구는 사용자가 초기 BitLocker 를 사용할 시에 설정된 48 자리의 숫자를 이용하는 방법이다. 사용자는 이 복구 암호를 다른 안전한 곳에 저장하거나, 프린트해서 보관하면 된다.

복구 키를 사용하는 방법은 외부 저장소로써 USB 플래쉬 메모리장치에 256 bit 키를 저장하는 방법으로 복구 과정에서 USB 를 인식하여 USB 저장장치에 저장된 복구키를 인식하게 된다.

AD 를 사용한 방법은 Microsoft 의 인증 서버를 사용하는 방법으로써 네트워크를 통해 연결되었을 시, 해당 TPM 의 복구 암호 및 복구 키를 원격 AD 서버에 저장하는 방법이다. 이 방법을 통해 저장된 복구 정보는 상위 AD 관리자 및 인증된 사용자에 의해 접근될 수 있다.

4. MTM 기반의 키 백업 시나리오

키 백업은 암호 시스템에서의 키 관리에 있어 필수적인 요로로 볼 수 있다. 특히 TPM 을 사용한 상용 솔루션으로써 BitLocker 가 나오게 되면서 앞으로 신뢰컴퓨팅기술을 사용한 보안 솔루션도 다양하게 나올 것으로 전망된다. 따라서 강력한 보안성을 제공하는 신뢰 컴퓨팅을 적용한 암호 시스템에서의 복구 시나리오 또한 매우 중요한 부분이라고 할 수 있다. 본 장에서는 모바일 환경의 신뢰컴퓨팅을 위한 MTM 을 사용하는데 있어 사용될 수 있는 키 백업 시나리오에 대해서 알아본다.

4.1 일반적인 키 백업 시나리오의 분류

여기서의 키 백업은 대상 암호키 K 를 백업하기 위해 사용되는 백업 키로써 BK(Backup Key)가 필요하며, 암호화된 키 $E_{BK}[K]$ 를 저장하는 저장공간이 필요하다. 따라서 BK 에 대한 생성과 EncKey 에 대한 저장 위치에 따라서 백업 시나리오를 분류할 수 있다.

① BK 의 생성을 사용자가 하고 백업 데이터도 사용자가 관리하는 시나리오

② BK 의 생성을 사용자가 하고 백업 데이터는 외부

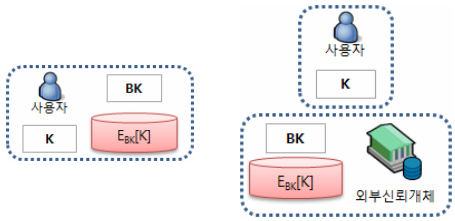

그림 1 일반적인 키 백업 시나리오 1/2

그림 2 일반적인 키 백업 시나리오 3/4

신뢰개체에서 관리하는 시나리오

③ BK 의 생성을 외부신뢰개체에서 하고 백업 데이터를 사용자가 관리하는 시나리오

④ BK 의 생성을 외부에서 하고 백업 데이터도 외부신뢰개체에서 관리하는 시나리오

위 네 가지 시나리오는 백업키 BK 의 관리와 암호화된 키의 저장소에 따라 분류를 하였다. 기본적으로 사용자에 의해 관리되는 것은 분실의 위험이 외부의 신뢰개체에 의해 관리되는 것 보다 높지만, 개인이 유연하게 접근할 수 있다는 것이 장점이다. 반대로 외부 개체에 의해 관리가 되는 것은 사용자에 의해 관리되는 것 보다 분실의 위험이 적고 안정적이지만, 유사시에 발생할 수 있는 데이터의 손상 및 분실에 대한 위험이 상대적으로 매우 크다. 이러한 특성 때문에 외부에서 관리하는 개체는 다양한 보안 위협에 대응할 수 있도록 높은 보안성을 가지고 있어야 한다. 그리고 부가적으로 해당 데이터에 대한 적법한 접근을 위해서 적절한 인증 절차를 제공해야 한다.

4.2 MTM 기반의 모바일 단말기의 키 백업 시나리오

MTM 을 사용하는 모바일 단말기에서는 단말기 내부 데이터 및 암호키 등을 보호하기 위해 MTM 을 사용한다. MTM 에서 사용하는 키의 구조는 (그림 3)과 같이 표현될 수 있다.

SRK 는 MTM 의 비휘발성 메모리 장치에 저장된 안전한 저장소를 위한 키이다. 이 키는 오직 MTM 내부에서만 사용할 수 있다. 따라서 이 *SRK* 를 사용하여 암호화 된 것은 해당 MTM 이 아니면 풀 수 없다.

SRK 로 암호화된 *USER Key* 는 모바일 단말기를 사용함에 있어 해당 사용자를 위한 키 관리를 위한 최상위 사용자키이다. 사용자가 생성하고 사용하는 모든 암호키는 *USER Key* 에 의해 암호화되어 관리되며 맨 아래 단의 키까지 상위 단의 키에 의해 보호를 받는다.

백업 대상의 키는 *USER Key* 이하의 키가 모든 키 혹은 특정 키가 될 수 있다. *USER Key* 에 의해 보호되는 키는 사용자의 인증 정보를 보호하고 있는 키나, 단말기상의 각종 어플리케이션에서 사용하고 있는 암호키, 혹은 컨텐츠에 적용된 인증 키일 수 있다. 따라서 모바일 단말에서 사용되는 MTM 관리 하에 있는 암호키들 및 인증서는 다음 (표 1)과 같이 분류될 수 있다.

여기서 MTM 내부에서 생성된 키의 경우에는 백업이 꽤 복잡할 수 있다. 왜냐하면 MTM 은 내부의 암호키를 외부에 노출시키지 않는 특성으로 인해 해당 암호키의 접근이 MTM 내부에서만 가능하기 때문이다. 이러한 키들은 TCG 의 Migration 을 사용하여 외부의 다른 TPM 객체에 이전하는 방법이나, 표준을 수정하여 해당 키를 외부에서 생성한 BK(Backup Key)로 암호화하고, 그 데이터를 다른곳에 안전하게 저장하는 방법, 그리고 외부의 신뢰 개체로부터 키를 전달받아 사용하는 방법이 있다.

암호키 및 인증서에 대해서 백업 시나리오는 다음 (그림 4)와 같이 제안할 수 있다. 여기서 백업 대상이 되는 정보는 MTM 의 관리 하에 있는 암호화된 키 체인인 Encrypted Key Chain 과 인증서인 Certification 이다. 사용자는 키 체인을 암호화한 루트키로써 *USER Key* 를 백업해야 한다.

표 1 MTM 관리하의 암호키 및 인증서의 분류

암호키	
MTM 내부 생성	MTM 외부 생성
- AIK, - SK(Storage Key), - AppKey(응용프로그램에서 사용)	- 사용자 정의키, - 이전된 외부키 - AppKey(응용프로그램에서 사용)
인증서	
MTM 내부 생성 인증서	MTM 외부 생성 인증서
- AIK 인증서 - 내부 전자서명 인증서 - 플랫폼 인증서	- 사용자 공인 인증서 - 신뢰된 프로그램 인증서 - 신뢰된 웹사이트 인증서

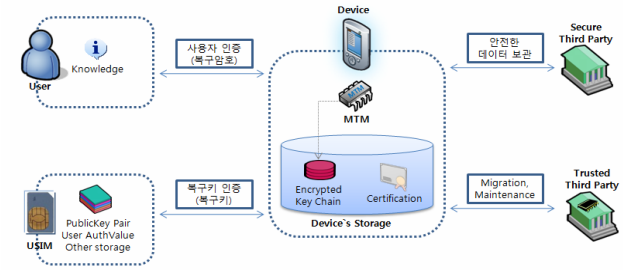

그림 4 MTM 기반 모바일 단말에서의 키 백업 시나리오

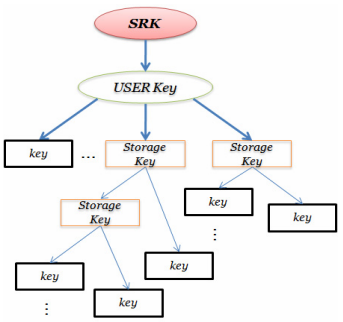

그림 3 MTM 의 키 관리 구조

USER Key 를 백업하기 위해서 MTM 내부 혹은 외부에서 BK 를 생성하고 *USER Key* 를 암호화하여 사용자 인증 모듈이나, 사용자에게 복구 암호를 표시하는 방법이 있다. 암호화된 데이터는 단말기의 저장소 및 외부의 안전한 저장소에 저장할 수 있는데, 이때 외부의 저장소가 TPM 을 가지고 있다면 Migration 이나 Maintenance 를 사용할 수 있다. 복구과정은 사용자의 복구 암호 및 USIM 의 복구 키를 사용하여 단말의 내부 혹은 외부의 개체로부터 암호화된 복구정보를 가져와 키를 복구할 수 있다.

5. 결론

신뢰컴퓨팅은 현재의 다양한 보안 위협요소를 보다 적극적으로 대응할 수 있는 보안 기술이다. 하지만 강한 보안 성을 제공하는 만큼 유연하지 못한 키 관리의 속성에 대해서 단말의 이동성 및 사용자에게 적절한 복구 프로세스를 제공해야 한다. 본 논문에서 분석한 MTM 기반의 키 백업 방안에 대해서 보다 면밀한 프로토콜의 설계와 보안성에 대한 분석이 향후 연구 방향으로 사료된다.

참고문헌

[1] Microsoft, "Windows Vista BitLocker Drive Encryption: Technical Overview", http://technet.microsoft.com/en-

us/windowsvista/aa906017.aspx
[2] Trusted Computing Group, "Mobile Trusted Module Specification General Overview FAQ," 2007.
[3] Trusted Computing Group, "TCG Specification Architecture Overview," Revision 1.4, 2007.