신뢰 컴퓨팅과 TCG 동향

Trusted Computing & Trusted Computing Group Standardization Trends

u-IT839의 정보보호 이슈 특집

김영수 (Y.S. Kim) 무선보안응용연구팀 선임연구원
박영수 (Y.S. Park) 무선보안응용연구팀 책임연구원
박지만 (J.M. Park) 무선보안응용연구팀 선임연구원
김무섭 (M.S. Kim) 무선보안응용연구팀 선임연구원
김영세 (Y.S. Kim) 무선보안응용연구팀 선임연구원
주홍일 (H.I. Ju) 무선보안응용연구팀 선임연구원
김명은 (M.E. Kim) 무선보안응용연구팀 연구원
김학두 (H.D. Kim) 무선보안응용연구팀 연구원
최수길 (S.G. Choi) 무선보안응용연구팀 연구원
전성익 (S.I. Jun) 무선보안응용연구팀 팀장

목 차

최근 몇 년 동안 컴퓨터 업계에서는 신뢰 컴퓨팅, 특히 TCG가 내놓은 새로운 표준에 대한 필요성과 기능, 그리고 새로운 가능성이 큰 이슈가 되어 왔다. TCG는 세계 IT 업계의 핵심 기업들이 중심이 되어 설립된 비영리 업계 단체로서 PC를 필두로 컴퓨팅 환경의 보안성 향상을 목표로 하고 있고, 이에 따른 여러 제품들이 출시되고 있다. TCG 관련 제품 중 특히 TPM을 탑재한 PC 및 handheld PC가 국내 시장에서도 보급되고 있고, 전세계적으로는 연간 5천만 대 이상이 TPM을 채용하고 있다. 이제 신뢰 컴퓨팅을 적용할 다음 목표는 임베디드 시스템 분야가 될 것으로 전망된다. 본 고에서는 신뢰 컴퓨팅의 개념을 설명하고 TCG의 최근 동향과 애플리케이션을 살펴본다. 그리고, TCG에 속한 다양한 워킹 그룹들 중 특히 모바일 폰 워킹 그룹(MPWG)에 대하여 고찰한 후 결론을 맺는다.

I. 신뢰 컴퓨팅의 필요성

컴퓨팅 디바이스의 외부 위협이 날로 증가하고 휴대하는 기기들이 소형화 및 대용량화 되면서 클라이언트 측에 쉽게 액세스할 수 있는 수단이 발달되어 다양한 보안 위협에 노출되고 있다. 특히 무선 통신 기술이 발달함에 따라 유선 상의 컴퓨팅 환경에서의 보안 문제점이 다음과 같이 무선 상으로도 확산되고 있다.

- 바이러스나 웜 감염에 의해 플랫폼보안 메커니즘을 공과(bypass)하거나 주요 데이터들이 조작될 수 있음
- 의도적인 서비스 거부(DoS) 공격을 통하여 네트워크 속도나 서비스의 질이 저하되거나 네트워크 자체가 마비될 수 있음
- 통신 선로 상에 공격자가 존재하면서 양방향으로 전달되는 정보들을 중간에 가로채어 조작한 후 인가된 사용자인 것처럼 프로토콜에 참여하는 man-in-the-middle 공격이 가능함
- 모바일 전자상거래 등을 통한 거래 데이터를 조작하여 이용자들에게 금전적인 피해를 입힐 가능성이 있음
- 주소록이나 신원 정보 같은 개인의 중요한 정보에 허가 받지 않은 상태로 액세스하거나 복제하는 등의 프라이버시 침해 위협
- 관련 장비들에 대한 물리적 공격으로 인해 서비스 자체를 제공받지 못할 가능성이 있음
- 신상 정보나 주소록 같은 개인 정보들이 비인가자에 의해 유출되어 오남용될 가능성이 있음
- 전자 티켓 복제나 불법 복제 소프트웨어 사용 등을 통한 저작권 침해 위협
- 작고 휴대가 간편한 디바이스를 사용하므로 이에 대한 도난 및 분실의 위협이 있음

Ⅱ. TCG

PC 업종의 대기업들은 새로운 하드웨어 접근 방식을 통해 관련된 산업 표준을 만들어 위와 같은 문제점을 해결하기 위해 컨소시엄을 구성하였다. 1999년에 Compaq, Hewlett-Packard, IBM, Intel 그리고 Microsoft 이렇게 5개 업체가 TCPA를 결성하였다[1]. 결성 목적은 네트워크, 통신, 그리고 전자상거래 같은 중요한 애플리케이션을 더욱 신뢰할 수 있도록 하기 위해 PC, PDA 또는 모바일 전화기 같은 신뢰할 수 있는 클라이언트를 만드는 것이었다. 또한, 동시에 관련 기술자들과 관심 그룹들에게 적절한 시기에 정보를 주고 신뢰를 얻기 위하여 이 표준은 가능한 한 공개된 상태로 유지되었다. 신뢰 컴퓨팅 표준은 하나의 LSI 보안칩 형태인 TPM을 메인 컴포넌트로 갖는 안전한 하드웨어 구조를 적용한다[2]. 이 표준은 고수준의 안전성을 갖는 스마트카드와 그 애플리케이션에 대한 경험을 토대로 하고 있다. 민감한 개인 정보나 비밀 데이터뿐 아니라 안전성이 요구되는 과정 보호를 위해 사용하는 스마트카드 암호 메커니즘을 TPM에 적용하여 플랫폼 무결성뿐 아니라 사용자 데이터 보호를 위해서도 사용한다. 엄밀히 말하여 TCG 표준은 사용자가 아닌 플랫폼을 위한 인증(authentication)과 인가(accreditation)를 제공한다.

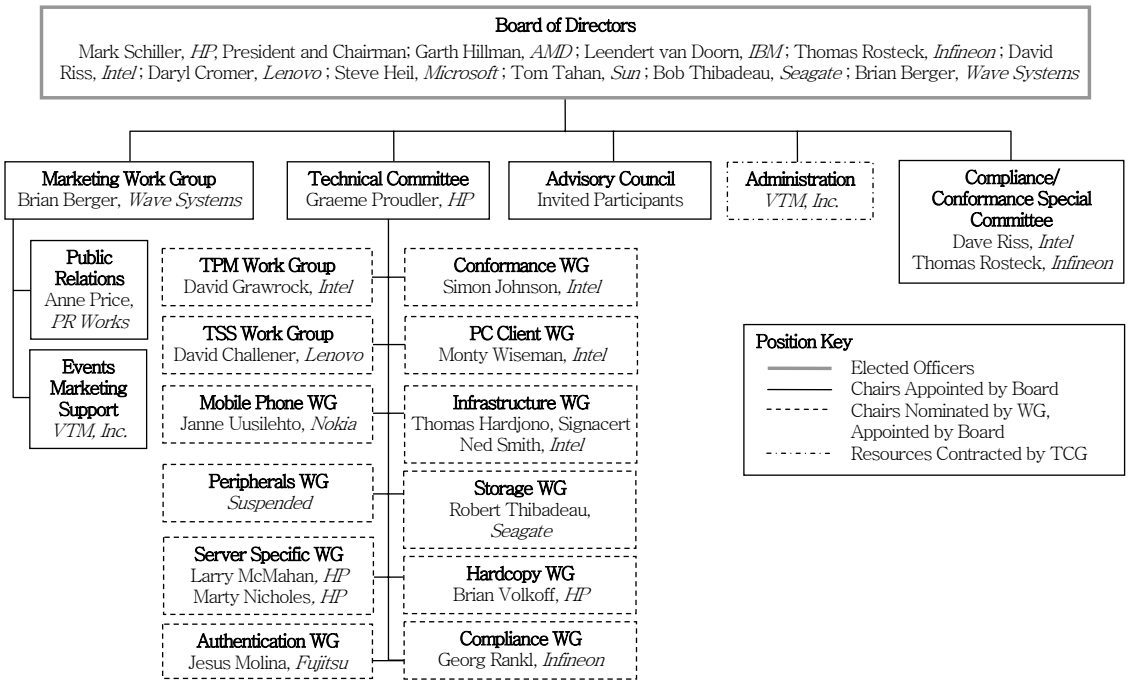
1. TCG 구성

TCG는 (그림 1)과 같이 몇몇 중심 기업들의 대표로 구성되어 정책을 결정하는 BoD 산하에 여러 개의 워킹 그룹(working group)과 기술 위원회(technical committee) 등을 두고 있다. 이 중 기술위원회는 BoD를 보좌하는 역할로써, 호환성과 상호

● 용 어 해 설 ●

TPM (Trusted Platform Module): TPM은 키와 패스워드, 그리고 디지털 인증서를 저장하는 일종의 마이크로 컨트롤러로, 외부 소프트웨어 공격이나 물리적 공격으로부터 저장된 정보를 안전하게 보호한다.

TCG (Trusted Computing Group): TCPA (Trusted Computing Platform Alliance)의 후신인 TCG는 신뢰 컴퓨팅 산업 표준을 개발하고 지원하기 위해 구성된 조직으로 현재 150개 업체들이 참여하고 있다.



(그림 1) TCG 구성

연동성 관점에서 각 워킹 그룹들이 작성중인 기술 스펙들을 모니터링하고 조언한다.

TPM 워킹 그룹은 TPM 스펙을 만드는 것을 목적으로 한다. 본 워킹 그룹과 기술위원회가 함께 TPM 구조를 정의한다. TSS 워킹 그룹은 TPM을 이용하고자 하는 애플리케이션 벤더들을 위해 표준화된 API 셋을 제공하는 역할을 한다. PC 클라이언트 워킹 그룹은 TCG 컴포넌트를 사용하는 PC 클라이언트들을 위해 일반적인 기능성이나 인터페이스, 그리고 최소한의 안전성 및 프라이버시 요구사항을 제공하는 것을 목적으로 한다. Mobile phone 워킹 그룹은 개방형 터미널 플랫폼 마켓에서 다양한 비즈니스 모델링을 위해 모바일 디바이스에 TCG 개념을 도입하는 작업을 진행중이다. 본 워킹 그룹에 대한 사항들은 별도의 장을 통해 좀 더 상세하게 기술한다. Peripherals 워킹 그룹은 플랫폼 주변 기기들의 신뢰-관련 속성들을 도출하고, 이러한 주변 기기들이 동작하는 다양한 환경을 조사하여 멀티-컴포넌트 신뢰 플랫폼 상에서 주변 기기의 역할과 영향을 좀 더 잘 이해하기 위해 구성되었다. Server 워킹 그룹은 서버에 TCG 기술을 구현하는 데 필요한 정의, 스펙, 가이드라인, 그리고 기술적인 요구 사항들을 제공하는 데 그 목적이 있다. Storage system 워킹 그룹은 기존의 TCG 기술과 철학을 굳건히 하고, 특히 스토리지 시스템에 대한 보안 서비스 표준을 중점적으로 다루고 있다. Hardcopy 워킹 그룹은 하드카피 에코시스템의 컴포넌트들을 위한 벤더 독립적 기술 스펙을 정의한다. Infrastructure 워킹 그룹은 개방형 플랫폼 구조 상의 다양한 비즈니스 모델링이 가능하도록 TCG 플랫폼별 스펙들을 인터넷과 엔터프라이즈 기반 구조에 적용하고 통합하기 위한 작업을 한다. Infrastructure 워킹 그룹 산하의 trusted network connect 서브 그룹은 네트워크 운영자가 종단 무결성에 관한 정책을 강화할 수 있도록 개방된 솔루션 구조를 정의하고 촉진시키는 데 그 목적이 있다. Conformance 워킹 그룹은 TPM의 PP에 대한 CC를 제공하는 것을 목적으로 한다. 여기서 PP는 TPM이 감내할 수 있는 위협 요소를 말한다. Compliance 워킹 그룹은 TCG 관련 제품들이 기능적으로 정확하고 완전하고 상호운용적으로

만들어졌는지를 평가 및 확인하기 위한 메커니즘을 제공하기 위해 만들어진 워킹 그룹이다. Marketing 워킹 그룹은 말 그대로 TCG를 홍보하기 위한 그룹으로 전 세계의 관련 학회에 참석하여 TCG를 알리거나 각 학교에 교육 코스를 개설하는 등 다양한 방법으로 TCG를 홍보하고 있다.

TCG는 매년 4회의 전체 미팅을 갖고 워킹 그룹별로는 전화 미팅(TelCo) 등의 방법으로 매월 1, 2회 정도 스펙 작성과 관련한 기술 협의를 한다. 2006년 11월에 미국 샌안토니오에서 개최되었던 TCG 연례 미팅에서는 각 워킹 그룹별로 심층 있는 토의가 이루어졌으며, 특히 이번에 새로 구성된 authentication 워킹 그룹에 대한 상세한 소개가 있었다. 본 워킹 그룹은 현재 스마트카드나 생체인증 등 인증 방식이 다양해짐에 따라 이러한 각종 인증 디바이스와 TPM간의 통신을 표준화하고자 구성된 워킹 그룹으로, 앞으로 쓰임새 모델과 위협 분석을 기반으로 한 스펙을 작성하고 TPM과의 인터페이스를 구현하는 것으로 향후 목표를 잡고 있다.

2. TCG 스펙

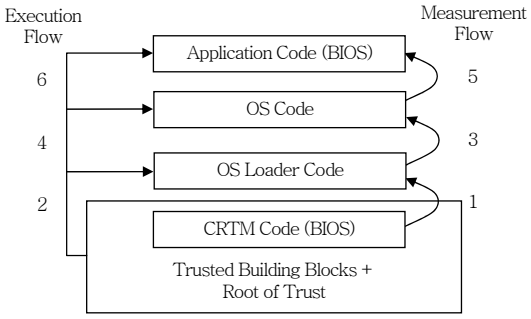
TCG는 130개 이상의 IT 업체들로 이루어져 있는 산업 표준 그룹으로 PC나 서버부터 모바일 디바이스나 주변 장치까지 다양한 컴퓨팅 디바이스를 아우르는 표준을 제공한다. TCG는 지금까지 6개의 메인 스펙을 발표하였다[3].

- Trusted Platform Module Specifications
- Infrastructure Specifications
- PC Client Specifications
- TPM Software Stack Specifications
- Trusted Network Connect Specifications
- Server Specific Specifications

위의 6가지 스펙은 새로운 안전한 플랫폼 상의 보안 컴포넌트를 위해 반드시 필요한 것들이다. TCG 멤버 회사들은 첫번째 구현이 유효하고 TPM 장착 신뢰 마더보드가 제품에 탑재될 준비가 되었다는 것을 확인하기 위해 매우 많은 자본을 투자해왔다. 또한, 20여 개의 워킹 그룹들이 차기 애플리케이션 옵션과 인터페이스를 준비하고 표준화하기 위해 작업중에 있는 등 표준화 작업도 동시에 병행하고 있다.

3. TCG 스펙의 보안 측면

지금까지의 보안이 추가적인 수준의 암호화나 안티 바이러스 소프트웨어에 의해 제공되었던 반면, TCG는 TPM이 직관적으로 신뢰받을 수 있는 가장 낮은 레벨인 시스템 부팅 과정으로부터 보안 기능을 제공한다. (그림 2)에서 보듯이 시스템 시작 시에 신뢰 체인(chain of trust)이 가장 낮은 계층으로부터 애플리케이션까지 차례대로 뻗게 된다. 각 경우의 바로 아래 레벨이 안전한 보안 레퍼런스를 갖게 되면, 다음 계층이 이를 지원받을 수 있게 된다. 하드웨어 보안 레퍼런스로서 TPM은 전체 체인의 "신뢰 근원(root of trust)"이 된다.



(그림 2) "신뢰 체인" 구조

Ⅲ. 암호 및 보안 메커니즘

신뢰할 수 있고 안전한 TC 요소들을 구현하기 위해서는 모든 주요 기능들이 기존의 검증된 보안 메커니즘들 중 하나를 사용해야 한다. 이에 백그라운드가 될 수 있는 암호 이론과 그 애플리케이션들을 아래에 기술하여 이해를 돕고자 한다.

암호학(cryptography)은 그리스어인 크립토스(kryptos)에서 온 것으로 숨겨진 것이라는 의미이다. 현대 암호학은 다음과 같은 4가지를 다룬다.

- 기밀성(Confidentiality): 정보는 의도하지 않은 사람이 해독할 수 있어서는 안된다.
- 무결성(Integrity): 정보는 스토리지에 있을 시에나 전송자와 의도된 수신자 간의 전송 시에 (변경 감지 없이) 변경되어서는 안된다.
- 부인 불가(Non-repudiation): 정보 생성자/전송자는 다음 스테이지에서 정보 생성 또는 전송에 대한 사실을 부인해서는 안된다.
- 인증(Authentication): 전송자와 수신자는 서로의 신원(identity)과 정보의 근원지/목적지를 확인시킬 수 있어야 한다.

부분적 또는 전체적으로 위의 4가지를 만족하기 위한 프로시저(procedure)와 프로토콜들을 암호시스템(cryptosystem)이라고 한다.

1. 암호 알고리듬

암호시스템의 핵심인 암호 알고리듬은 메시지 등의 입력 값을 취하고 이것을 특정 수학적 함수와 키를 통해 변형하는 기능들을 수행한다. 여기서 키는 이러한 함수들이 단일 출력 값을 내도록 제어한다. 이러한 기능을 수행하기 위해 두 가지 방법이 존재한다. 암호화(encryption)는 평문(plaintext)이라고도 하는 원본 메시지를 암호화된 형태로 변형하기 위해 암호키(cryptographic key)를 사용한다. 이와는 반대로, 복호화(decryption)는 암호화된 메시지를 원래 형태로 복원하기 위해 암호키를 사용한다. 키는 충분한 크기를 갖는 숫자이거나 일련의 비트들로서 시스템적 방법으로 추측하거나 발견할 수 없다. 이러한 키의 길이는 알고리듬의 형태와 해당 암호 강도에 따라 달라진다. (요즘에는 64비트부터 2048비트까지의 키가 사용된다.)

사용되는 암호키의 개수와 형태에 따라 두 가지 기본적인 암호 알고리듬 형태가 존재한다.

가. 대칭키 암호 알고리듬

대칭키(symmetric key) 암호 알고리듬은 암호화와 복호화에 하나의 비밀키를 사용하는 방식으로, 각 통신 참여자가 통신 초기화 전에 키에 접근할 수 있어야 한다.

나. 비대칭키 암호 알고리듬

비대칭키(asymmetric key) 암호 알고리듬은 관련된 키의 쌍을 사용하는 방식으로, 암호화와 복호화 시에 각각 다른 키가 사용된다. 비대칭키 암호 알고리듬은 보안 통신에 널리 사용되고 있다. 메시지 수신자가 자신의 첫번째 키를 공개하고 두번째 키는 자신의 제어 하에 비밀로 유지한다. (그러므로 첫번째 키를 공개키(public key), 그리고 두번째 키를 비밀키(private key)라고도 한다.) 이 수신자에게 암호화된 메시지를 보내고자 하는 참여자는 메시지 암호화를 위해 수신자의 공개키를 사용한다. 암호화된 메시지를 수신한 수신자는 자신의 비밀키를 안전한 저장소에서 꺼내어 복호화를 위해 사용한다. 만일 전송 시에 메시지를 누가 가로채더라도 비밀키 없이는 메시지의 내용을 읽을 수 없다. 이 알고리듬의 큰 장점은 통신을 시작하기 전에 안전한 통신로를 통해 키를 교환할 필요가 없다는 것이다.

다. 메시지 또는 데이터에 대한 디지털 서명

암호시스템의 두번째 목표는 양자 간에 전송되는 메시지들의 무결성을 보장하는 것이다. 무결성은 통신 송수신자들에게 메시지나 프로그램 같은 데이터 시퀀스가 변경되지 않았다는 확신을 제공한다. 무결성 보장을 위해 메시지 송신자는 메시지와 함께 해시 함수를 함께 전송한다. 여기서 해시 함수는 “메시지 다이제스트”라고 불리는 메시지의 축약을 생성하는 수학적 알고리듬이다. 수신자는 메시지를 복호화하고, 동일한 해시 함수를 이용하여 자신만의 메시지 다이제스트를 생성하여 메시지와 함께 전달되어 온 다이제스트와 비교한다. 만일 두 개의 다이제스트가 일치한다면 수신자는 메시지의 무결성이 유지되고 있음을 확신할 수 있다. 그러나, 두 개의 다이제스트가 다르다면 메시지의 어딘가가 변경되었다는 것을 의미한다. (이러한 변경은 전파 방해 같

은 의도적인 장난이나 불안정한 네트워크 디바이스로 인한 결과뿐 아니라 데이터 무결성에 대한 공격의 결과일 수도 있다.) 본 장의 도입 부분에 언급되었던 모든 보안 기본 메커니즘들을 수행하기 위해 다음과 같은 도구들을 갖게 되었다.

- 메시지의 기밀성 보호를 위해 수신자의 공개키로 메시지를 암호화
- 암호화된 메시지를 읽기 위해 메시지를 비밀키로 복호화
- 메시지의 디지털 서명을 생성하기 위해 메시지 다이제스트를 비밀키로 암호화
- 메시지의 디지털 서명을 검증하기 위해 송신자의 공개키로 디지털 서명을 복호화하고 이 결과를 계산한 메시지 다이제스트와 비교

2. 암호 인증서

전 장에서 언급된 알고리듬과 암호시스템의 주요 요소는 바로 키 그 자체와 키의 사용, 그리고 키의 취급이다. 특히 비대칭키 함수를 사용할 때에는 사용된 키가 누구를 지정하는 것이고 이것이 의심된 곳으로부터 온 가짜 키가 아니라는 것을 모든 사람들이 알 수 있도록 해야 한다. 이러한 단계를 위해 신뢰할 수 있는 키 박스인 인증서(certificate)가 모든 관련 표준들에 명시되어 있다.

디지털 인증서는 키와 다양한 정보들(근원지가 어디인가? 어떤 소유자를 위한 것이고 어떤 애플리케이션을 위한 것인가? 등)을 담고 있는 데이터 구조로서, 소위 신뢰 센터(PKI에서의 제삼자)에 의해 디지털 서명된 일종의 진품 증명서라고 할 수 있다. 디지털 인증서를 획득하고자 하는 서버나 사용자들은 Verisign™ 같은 잘 알려진 CA 중 하나와 접촉하여 이를 얻거나, 자신이 속한 IT 조직에 의해 이를 생성한다. CA는 인증서에 부여된 신뢰 수준에 따라 각기 다른 과정을 통해 인증서를 요구하는 객체로 하여금 자신의 신원을 증명할 것을 요구한다.

인증서 요구자의 신원이 확인되면 CA는 디지털 인증서를 발급한다. 이 인증서는 X.509 표준에 맞게 구성되어 있으며, CA의 이름, 인증서 소유자의 이름, 인증서 유효 기간, CA가 인증서를 서명하기 위해 사용한 알고리듬에 대한 상세 정보, 그리고 가장 중요한 인증서 주체의 공개키를 담고 있다. CA는 자신의 비밀키로 인증서를 서명하고 이를 인증서 주체에게 제공한다.

인증서 주체(사람이나 컴퓨터)는 다른 사용자나 시스템과의 보안 통신에 들어가기 전에 자신의 신원을 증명하기 위해 본 인증서를 사용한다. 주체가 인증서를 상대방에게 보내면 상대방은 CA의 비밀키로 생성된 서명을 검증하기 위해 CA의 공개키를 사용한다. 본 검증 과정이 성공하면 본 인증서의 수신자는 인증서에 저장된 주체의 공개키가 믿을 수 있음을 확신할 수 있게 된다. 수신자는 이 공개키를 사용하여 인증서 주체와의 비밀 통신 세션을 초기화한다.

수신자는 공개키 암호의 특성으로 인해 통신 과정이 안전함을 믿을 수 있다. 주체의 디지털 인증서에는 비밀이 없으며 자유롭게 분배될 수 있다. 만일 공격자가 본 인증서를 사용하여 인증서의 주체인 것처럼 속이려고 시도한다고 하더라도 그는 주체의 비밀키에 접근할 수 없으므로 주체의 공개키를 통해 초기화되는 통신 세션에 참여할 수가 없다.

Ⅳ. 신뢰 플랫폼과 TPM

1. TCG 스펙의 객체

TCG가 정의한 신뢰 플랫폼은 플랫폼 상의 신뢰 하드웨어/소프트웨어와 암호학적 증명 메커니즘에 사용하기 위한 외부 CA와의 연결 및 통합으로 구성된다. 다음은 플랫폼의 논리적 구성이다[4].

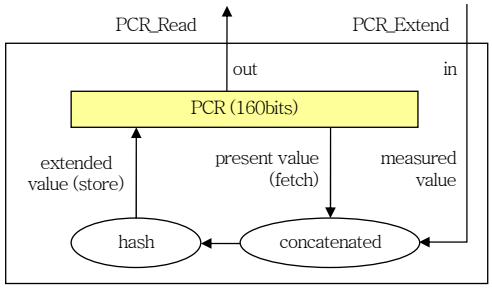
- TPM: 칩으로 구현된 하드웨어 보안 디바이스로서 모든 기본적인 신뢰 관련 연산들과 특히 암호 함수들이 안전하게 다루어진다. TPM의 구조는 디지털 서명이나 지불 트랜잭션에 사용되는 일반적인 고비도 스마트 카드의 구조와 대략적으로 상응한다.

- Core Root of Trust for Measurement (CRTM): 운영 체제가 적용되기 이전에 플랫폼이 부팅되자마자 실행되는 루틴들로 구성된다. 본 루틴은 부팅 과정의 무결성을 측정하고 모니터해서 안전한 스타트업 과정을 수행하기 위한 것이다. 기술적으로는 검사를 위해 TPM에 보내어지는 부분에 대한 해시 값을 생성함에 의해 이루어진다.
- Initial Program Loader (IPL): 운영 체제의 무결성을 보증하는 BIOS와 운영 체제 간의 링크이다.
- Trusted Platform Support Service (TSS): 표준화된 고수준 TPM 인터페이스(C로 레퍼런스된 API)를 포함한 운영 체제를 제공하는 것으로 운영 체제나 애플리케이션의 보안 함수를 다룬다.

2. TPM: 하드웨어, 소프트웨어, 기능

TPM은 TCG에 의해 제정된 산업 표준 규격을 기초로 한 보안 칩(security chip)으로 마이크로 컨트롤러, 암호 엔진, 표준 입출력 인터페이스, 안전한 메모리를 갖추고 공개키, 디지털 인증서, 암복호, RNG, 인증, 보증, 민감 데이터 보호 기능을 제공한다. 그리고, TPM은 저전력, 고성능 프로세서 설계 기술을 요구한다. TPM에 의해 다루어지는 주요 보안 기능은 다음과 같다.

- 키 보호: 다양한 키 클래스들이 보호된 형태로 TPM 내에 저장된다. 접근 방법은 키 타입에 의해 결정된다.
- 시스템 인증: 제삼자에 대하여 플랫폼을 인증하고 검증한다.
- 시스템의 보안 상태 통신 – 보증(attestation): 보안-관련 구성(configuration)에 대한 신뢰 통신
- RNG: 안전한 키 생성을 위한 하드웨어-기반 난수 생성
- 안전한 저장: (그림 3)에서와 같은 동작을 통해 PCR에서의 플랫폼 구성 변경을 안전하게 저장: PCR_n (new)←SHA-1(PCR_0||measurement)



(그림 3) PCR 동작

- 실링(sealing): 실링은 TPM의 매우 강력한 특징으로, 플랫폼이 정상적인 기능을 할 때에만 보호된 메시지의 내용을 복구할 수 있게 된다. 실링은 암호화된 메시지(실제로는 메시지를 암호화하는 데 사용하는 대칭키)를 PCR 레지스터 값들과 non-migratable 비대칭키에 결합시킨다. 일정 범위의 PCR 레지스터 값을 선택하고 PCR 값과 메시지 암호화에 사용된 대칭키를 함께 암호화하여 실링된 메시지를 생성한다. 플랫폼 구성이 메시지 전송자가 정한 PCR 레지스터 값과 같을 때에 한하여 TPM은 복호화키를 가지고 대칭키를 복호화 할 수 있다.

또한, TCG는 다음과 같은 고려 사항들도 강조하고 있다.

- TPM 무결성에 대한 공격, 특히 물리적 공격에 대한 보호
- 보급이 용이하도록 저렴한 비용으로 구현
- 신뢰 플랫폼에 대한 국제적 거래가 제한 받지 않도록 수출 규정과의 호환성(compliance) 제공

TPM 내의 암호/보안 하드웨어를 최소로 사용하여 구현할 수 있도록 시스템을 설계한다.

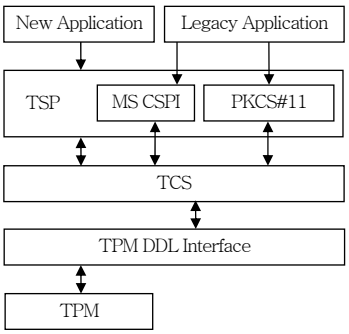
- 최고 2048비트까지 RSA 암호의 빠른 계산을 위한 암호 연산 기능
- 2048비트까지의 RSA 키 생성 기능
- SHA-1/HMAC 알고리듬을 위한 하드웨어 해시 기능
- True RNG 기능
- 해킹 방지 및 tamper evidence 기능

- 재전송 공격을 막기 위한 카운터
- 운영 전압 스위치가 꺼지더라도 데이터를 유지할 수 있는 비휘발성 메모리(EEPROM)
- 물리적인 공격과 이에 대한 대응을 위한 센서와 내부 보안 구조(예를 들면, 칩의 최상위 와이어 계층의 액티브 스크린)
- TPM 자체 테스트 함수

내부 펌웨어(firmware)는 표준에 의해 호스트 소프트웨어(TSS)에 정의된 인터페이스 프로토콜을 구현하고 이를 위해 위에서 언급한 하드웨어 함수들을 사용한다. 또한, 펌웨어는 다양한 보안 센서들을 체크하고 관리할 뿐 아니라, 칩이나 그 환경에 대한 물리적 위조 또는 변경이 감지되면 정확하게 반응한다. 구현의 정확성은 독립적인 테스트 기관이 체계적인 인증 과정을 통해 체크하고 확인한다.

V. TC 소프트웨어 스택

다른 하드웨어 구성요소들과 마찬가지로, TPM은 특정 드라이버와 서비스 제공 인터페이스를 필요로 한다. 이러한 신뢰 플랫폼 지원 서비스(TSS)는 관련 운영 체제에 TPM 함수들을 제공하는 보안 API로 구성된다. TSS의 목적은 애플리케이션에게 TPM 기능에 대한 단일 엔트리 포인트를 제공하고, TPM에 대한 동기화된 액세스를 제공하며, 명령어 스트림을 정확한 바이트 오더링으로 숨기고, TPM 리소스를 관리하는 것이다. (그림 4)는 TSS의 구조를 나타낸 그림이다.



(그림 4) TSS 구조 다이어그램

최하위 레벨에서 TSS는 인터페이스를 초기화하고 LPC 버스를 통해 TPM과 데이터를 교환하는 하드웨어-기반 디바이스 드라이버(커널 모드)로 구성된다. 그 다음 상위 레벨은 다음과 같은 시스템 서비스로 구성된다.

- TPM Device Driver Library (TDDL): TDDL은 TPM 애플리케이션에 대하여 운영체제 독립적인 인터페이스를 제공하며, 여러 TSS 구현들이 어떠한 TPM과도 정확히 통신할 수 있도록 한다.
- TSS Core Services (TCS): TCS는 일반 플랫폼 서비스들에 대한 인터페이스를 제공한다. 하나의 플랫폼에 여러 개의 TSP가 있다고 하더라도, TCS는 모든 TSP들이 정상적으로 동작하도록 한다. TCS는 다음과 같은 핵심 서비스를 제공한다.
  - Context Manager: TPM에 대한 threaded 액세스
  - Credential & Key Management: 플랫폼과 관련된 인증서와 키를 저장
  - Measurement Event Management: 이벤트 로그 엔트리와 PCR 레지스터와 연관된 액세스를 관리
  - Parameter Block Generation: TPM 명령어들에 대한 serializing, synchronizing, processing을 책임짐
- TSS Service Provider (TSP): TSP는 TPM에 대한 C 언어 인터페이스를 제공하며, 애플리케이션과 동일한 프로세스 주소 공간에 존재한다. 신원 확인(authorization)은 본 계층의 사용자 인터페이스나 TCS 계층의 callback 메커니즘을 이용하여 본 계층에서 수행된다. TSP는 콘텍스트 관리 서비스와 암호 서비스를 제공한다. 콘텍스트 관리 서비스는 애플리케이션과 TSP 리소스를 효과적으로 사용하기 위한 핸들을 제공하

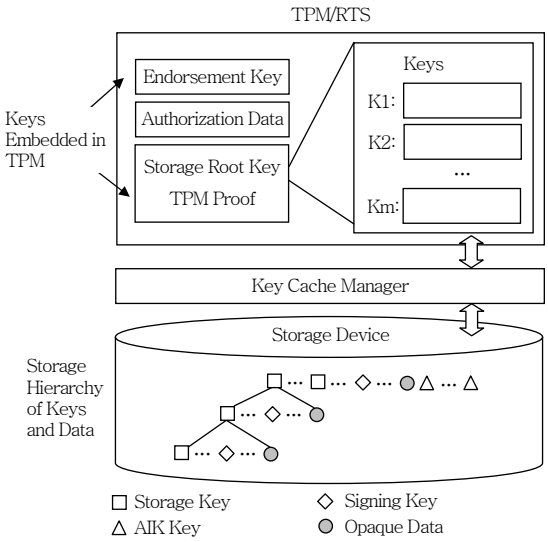
며, 암호 서비스는 TPM 보호 기능을 효율적으로 사용하기 위해 암호 기능을 제공한다. 두 개의 표준 API가 적용될 수 있다.

- MS Cryptographic Service Provider (CSP): Outlook®, Explore, Word 같은 Windows® 상의 다양한 애플리케이션 프로그램들은 암호화나 서명 같은 보안 함수들을 담고 있고, 이러한 함수들은 그들만의 암호 인터페이스인 MS-CAPI를 통해 다루어진다. MS-CAPI는 소프트웨어 모듈, 암호 토큰 또는 TSS 같은 다양한 보안 프로바이더에 액세스하는 방법으로 TPM에 의해 관리될 수 있다. 그러므로, 이미 MS_CAPI를 사용하고 있는 기존 보안 애플리케이션들을 타 CSP 선택을 통해 TPM의 상위 보안 계층에 포팅하는 것은 상대적으로 용이하다.
- PKCS#11: RSA사가 개발한 PKCS#11은 가장 널리 사용되고 있는 보편적인 암호 인터페이스 표준으로, 예를 들면 Netscape 브라우저에 사용된다. PKCS#11 보안 호출을 TSS-API로 변환하는 것은 기존 표준 애플리케이션 적용을 용이하게 한다. 그러므로, TPM 내에 브라우저를 위한 인증서들을 안전하게 저장함으로써 최소한의 구현 비용/복잡도로 고수준의 보안 솔루션들이 만들어질 수 있다.

Ⅵ. 스토리지 보호

스토리지 신뢰 근원(RTS)은 TPM에 위임된 키와 데이터를 보호한다. RTS는 서명과 복호화 과정을 수행하는 동안 키들을 갖고 있는 작은 휘발성 메모리를 관리한다. 활성화된 다른 키들에게 공간을 만들어 주기 위해 비활성화된 키들은 암호화되어 칩 외부로 옮겨진다. 키 슬롯 캐시 관리는 TPM 외부에서 KCM에 의해 수행된다.

KCM은 비활성화된 키들이 저장된 스토리지 디바이스와의 인터페이스를 갖는다. TPM과 관련된



(그림 5) RTS 구조

키로는 AIK와 서명키, 그리고 스토리지키가 있다. (그림 5)에서 보듯이, SRK와 EK는 TPM에 임베디드 된다. EK는 TPM 칩 조립의 마지막 단계에 TPM 내에 생성되는 2048비트의 비밀키/공개키 쌍이다. 비밀키는 더 이상 읽을 수 없을 뿐 아니라 TPM에서만 내부적으로 사용될 수 있다. SRK는 소유권 획득 과정(take ownership)을 통해 소유자에 의해 자동으로 생성된다. SRK는 안전하게 저장된 낮은 순서의 키나 데이터들을 포함한 키 계층 구조의 루트에 있으므로 이러한 키나 데이터들의 신뢰성은 SRK에 의존한다. SRK는 TPM 외부에 저장된 키들을 보호하는 데 사용된다.

1. 키 속성

RTS가 관리하는 모든 키들은 migratable 또는 non-migratable 속성을 갖는다. 이러한 키 속성은 키가 TPM에서 다른 TPM으로 전송될 수 있는지 여부에 따라 결정된다. 속성값은 키가 생성될 때 셋업되고 이후에는 변경되지 않는다. Non-migratable 키는 특정 TPM 인스턴스와 영속적으로 결합되어 있어서, 이 키의 migration은 특정 플랫폼이 다른 플랫폼과 같은 것처럼 보이는 효과를 갖게 된다. AIK는 migration 될 수 없는 대표적인 예로써 non-

migratable로 고정된다. Migratable 키는 TPM 디바이스 사이에 교환될 수 있으므로 사용자가 이용한 디바이스에 관계 없이 사용자와 키 쌍이 함께 움직일 수 있다. 사용자들 사이에 교환된 메시지들은 컴퓨팅 플랫폼이 바뀌더라도 액세스 가능 형태로 남아 있게 된다. 키 속성은 일반 데이터에는 적용되지 않는다. Non-migratable 속성을 일반 데이터로 확장하기 위해서 데이터는 non-migratable 스토리지 키를 사용하여 RTS와 함께 저장되어야 한다. 일반 데이터들이 TPM의 제어 하에 있는 한 어떤 곳에서도 복호화되지 않으나, 일단 데이터가 TPM 외부에서 복호화되고 나면 다른 시스템에 migration 될 수 있다.

2. 외부 스토리지와 KCM

TPM은 제한된 런타임과 비휘발성 스토리지를 갖는 저비용 컴포넌트이나 TCG 사용 시나리오 상에서는 무제한의 스토리지가 요구되므로 TPM 외부 스토리지와 KCM 개념이 필요하다.

키와 스토리지를 위한 무제한적인 공간을 확보하기 위해 RTS는 외부 스토리지에 있는 키들을 암호화된 키 BLOB으로 패키징한다. 키 BLOB은 TPM 외부에서는 일반적인 데이터로 인식되므로 플래시나 디스크 또는 NFS 등 어떠한 스토리지 디바이스에도 저장될 수 있다. BLOB은 핸들이나 또는 다른 적절한 레퍼런스 메커니즘에 의해서 자신의 내용에 대한 해시 값을 통해 참조된다. 레퍼런스 식별자(identifier)는 외부적으로 KCM이나 스토리지 기능을 수행하는 애플리케이션 프로그램에 대하여 BLOB을 명확히 해준다.

TPM은 외부 프로그램이 TPM의 제한된 스토리지 리소스를 관리할 수 있도록 하는 인터페이스를 갖는다. 키를 캐시하는 기능과 키를 사용하는 기능을 분리함으로써 관리 기능은 애플리케이션 기능과 구별된다. 애플리케이션들이 키 사용에 관련되어 있는 반면에, KCM은 일반적으로 키 캐싱에만 관여한다. 다만 다른 키들을 보호하는 데 사용하는 스토리지 키의 경우는 예외로, KCM은 이러한 스토리지 키 사용도 제어한다.

(그림 5)에서 KCM은 TPM의 휘발성 키 슬롯 메모리와 비휘발성 외부 스토리지 디바이스 사이에서 키 움직임을 다루는 외부 프로그램으로 나타내어져 있다. KCM은 유효한 키 슬롯을 찾다가 적절한 때에 키를 방출하고 다른 것으로 대체한다. TPM은 키 슬롯이 비거나 애플리케이션이 특정 키를 사용하고자 할 때 이에 대하여 사전에 통지하지 않으므로 애플리케이션 프로그램은 이 같은 이벤트가 일어났음을 KCM에게 알려줄 필요가 있다.

Ⅶ. 기능과 애플리케이션

1. 보안 기능

TPM API인 TSS는 플랫폼 운영 체제와 애플리케이션 프로그램을 위한 보안 서비스를 제공한다. TSS 고유 API가 운영 체제 관련 작업들의 실행을 위한 것인 반면, MS-CAPI나 PKCS#11 같은 보편화된 암호 인터페이스는 애플리케이션을 위한 것이다. 그러므로 하드웨어 상에 암호 기능들을 안전하게 구현하거나 키 소재 또는 다른 민감 데이터들을 안전하게 관리하는 것이 가능하다. TPM과 TSS는 각 사용자들마다 구분된 독립적인 보안 환경을 구축할 수 있다.

2. 무결성 확인

소유권 획득(taking ownership) 과정을 통해 소유자는 PC나 노트북의 신뢰 상태를 구축할 수 있다. 다음 부트 과정 동안, 시스템은 현재 상태를 TPM의 PCR 레지스터에 저장된 레퍼런스 상태와 비교하여 같은지를 확인하고, 같다고 확인이 되면 이를 신뢰하게 된다. 공격이나 바이러스 등으로 인한 중요한 부분의 변조는 이러한 과정을 통해 감지될 수 있고 사용자는 이에 대하여 적절한 조치를 취할 수 있게 된다.

3. 인증

안전한 전자상거래나 제한된 웹 페이지 액세스에 이용하기 위해, 키 쌍이나 인증서가 TPM 내에 저장될 수 있다. 이를 통해 은행 같은 상대방에게 자신의 신원을 증명할 수 있고 동일한 메커니즘을 통신 암호화에 사용할 수도 있다. 또한, 방화벽이나 VPN에 대한 안전한 원격 제어나 모니터링에도 활용될 수 있다.

4. 시스템 관리

TPM의 도움으로 시스템 관리자는 관리하고 있는 네트워크 상에 다른 디바이스들을 명백하게 구분해 낼 수 있다. 새로운 디바이스들은 네트워크 관리를 통해 기록되므로 알려지지 않거나 변형된 디바이스들은 바로 감지된다. 이를 통해 보안 정책들이 더욱더 자동화되고 제어 가능 모드로 구현될 수 있다. 기존의 원격 접근 서버 과정을 통해 사용자들의 신원 증명 정보(이름, 패스워드, 스마트카드, 생체인식 등)뿐 아니라 사용된 플랫폼도 알 수 있다. 네트워크는 사용자의 접근 권한이나 회사 노트북이 시스템에서 사용되고 있는지 여부, 또는 노트북이 신뢰 상태인지 여부 등을 확인할 수 있다. 이러한 확인 과정을 통과하게 되면 보안 정책은 제한 없이 접근이 가능하도록 허가한다. 만일 인가된 사용자가 미확인된 PC를 사용할 경우에는 파일 접근 같은 제한된 권한의 동작만이 가능하게 된다.

5. 익명성 제공

보증 과정을 통해 TC 플랫폼은 익명의 신원을 가진 상태로 존재할 수 있다. 조달이나 경매 플랫폼에서 구매자가 입찰자의 신원에 영향 받지 않고 익명의 입찰을 진행할 수 있도록 하는 경우가 하나의 예가 될 수 있다. 외부의 신뢰 센터는 익명의 신원과 실제 신원간의 연결 정보를 가지고 있어야 한다. 입찰이 수락된 후, 신뢰 센터는 상호 신원에 대한 정보를 제공하게 되고 이를 통해 계약이 성사된다.

Ⅷ. 향후 애플리케이션

TCG가 PC 보안에 관한 활동으로 시작했지만 안전한 플랫폼에 대한 아이디어는 다른 디바이스와 애플리케이션들로 전이되고 있다. TCG 프레임워크 내에서 다양한 애플리케이션 분야의 워킹 그룹들이 생겨났으며 발빠르게 움직이고 있는 상황이다. 이 중 몇 가지 주요 논의 주제를 살펴보면 다음과 같다.

• PDA와 스마트 폰

현재 PC와 유사한 특징과 기능들을 가지고 있는 PDA는 인터넷 상에서 지속적으로 운영되어야 하고, 휴대가 간편한 특징으로 인해 도난과 분실의 위험이 존재한다. PDA의 운영체제는 최소한의 보안 기능을 갖거나 아예 갖고 있지 않다. 디바이스 손실은 포함하고 있는 모든 데이터들이 손상되었을 경우에 기인한다. TPM을 적용하게 되면 인증 및 암호화 방법을 통해 상당한 안전성 향상을 기대할 수 있다.

• 모바일 통신 애플리케이션

UMTS와 같은 현대적 디바이스들이 운영되고 있고 역시 1년 365일 내내 인터넷에 연결되어 있으나, 지금까지 특정 보안 관련 예방책들은 도입하고 있지 않다. TPM을 적용하면 데이터 안전성이 향상될 뿐 아니라 가능한 애플리케이션들도 상당수 많아질 것으로 예상된다. 특히, 안전하게 인증서를 디바이스에 저장할 수 있는 능력은 새로운 신뢰 애플리케이션을 가능하게 할 것이다. 유해한 소프트웨어로 인해 증가되는 위험도 TC-기반 운영 체제를 사용함에 의해서 적절하게 대비할 수 있다.

• 통신(WLAN 보안, 네트워크 원격 액세스 등)

WLAN의 제1세대 시스템들은 점점 늘어나는 견고한 보호 메커니즘들로 교체되고 있고, 키 소재의 안전한 저장과 디바이스 인증서의 저장에 대한 요구사항이 생겨나고 있다. TPM은 WLAN 공중 인터페이스뿐 아니라 RADIUS나 DIAMETER 같은 네트워크 접근을 위해 신뢰성을 보장하는 형태로 디바이스에 보안을 통합하도록 할 수 있다.

• 디바이스 보안과 무결성

무결성과 불법 변경 등의 공격에 대해 자산의 보호를 위해 많은 애플리케이션들이 출현하고 있다. 이러한 애플리케이션은 엔진 제어 같은 자동차 디바이스나 마일리지 등의 중고차 가격 관련 파라미터들을 보호하는 것으로부터 화학 공장 등의 시스템 제어기를 보호하는 것까지 매우 다양하다.

Ⅸ. MPWG 표준화 동향

MPWG는 개방형 터미널 플랫폼 마켓에서 다양한 비즈니스 모델링을 위해서 모바일 디바이스에 TCG 개념을 도입하는 것을 목적으로 한다. 본 장에서는 MPWG에서 정의한 쓰임새 모델을 살펴보고, 신뢰 모바일 플랫폼과 모바일 TPM에 대하여 알아본다.

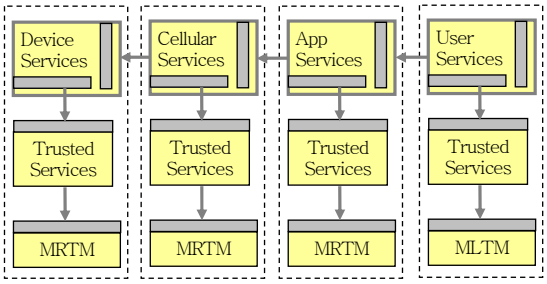
1. 쓰임새 모델

다음은 모바일 디바이스를 사용하는 환경에서 TCG를 통해 보안성을 제공하기 위한 쓰임새 모델들이다.

- 사용자 데이터 및 프라이버시 보호: 개인 신원 정보나 주소록 같은 사용자의 개인 정보에 비인가자가 접근하거나 도용하는 것을 막음
- 플랫폼 무결성: 허가된 운영 체제와 하드웨어를 통해서만 디바이스 동작이 이루어지도록 함
- 디바이스 인증: 사용자를 인증하고 디바이스 신원 그 자체를 증명함
- Robust DRM 구현: 사용자가 획득하고 콘텐츠나 서비스 제공자가 필요로 하는 데이터를 보호하기 위해 DRM 구현물이 신뢰를 얻을 수 있도록 함
- SIMLock/디바이스 personalization: 허가 과정을 통해 모바일 디바이스가 unlock 상태로 될 때까지 특정 네트워크나 서비스 제공자에 대하여 모바일 디바이스가 lock 되도록 함
- 안전한 소프트웨어 다운로드: 애플리케이션 소프트웨어나 업데이트, 펌웨어 업데이트 또는 공격 방지를 위한 패치 등을 안전하게 다운로드 하도록 함
- 디바이스와 UICC간 안전한 채널: 디바이스와 UICC에 각각 부분적으로 구현되어야 하는 모바일 전자 상거래 같은 안전성이 중요시되는 애플리케이션들에게 공유된 기능을 제공
- 모바일 티켓팅: 사용자가 모바일 디바이스에 전자 티켓을 구입하여 다운로드 받고 이를 통해 각종 이벤트에 입장하거나 서비스에 접근할 수 있는 새로운 서비스 제공
- 모바일 지불: 모바일 디바이스가 전자 지불을 위한 사용자의 지갑으로 사용될 수 있도록 함. 신용 카드, 직불 카드, 선불 펀드, 온라인 계정 등 다양한 지불 방법 지원
- 소프트웨어 사용: 디바이스 사용자 정책에 따라 각종 공격에 대해 소프트웨어 애플리케이션들의 무결성을 유지하고 다른 디바이스 기능들에 방해 받지 않도록 함

2. 신뢰 모바일 플랫폼과 모바일 TPM

MPWG 스펙은 하나의 신뢰 모바일 플랫폼을 여러 개의 신뢰 엔진들로 추상화하는데, 이는 설계자가 하나 이상의 엔진을 지원하는 여러 프로세서들을 사용하여 플랫폼을 구현하도록 하기 위함이다. 일반적인 신뢰 모바일 플랫폼을 예시한 (그림 6)은 각기 다른 stakeholder들에 따라 여러 개의 추상 엔진을 포함하고 있다. (플랫폼 소유자를 모바일 환경에서



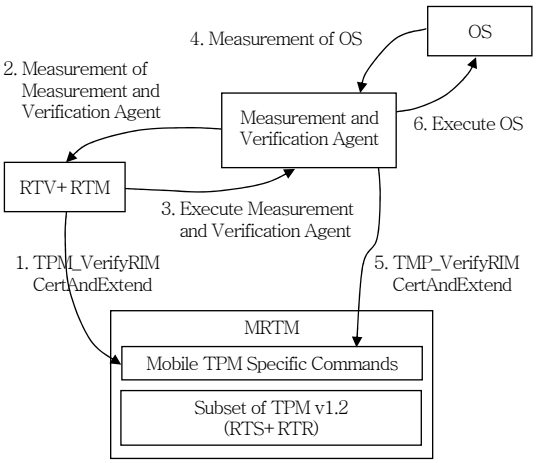
(그림 6) 일반 신뢰 모바일 플랫폼의 예

는 엔진에 대한 stakeholder라 칭한다.)

엔진들은 각기 디바이스, 셀룰러(cellular) 액세스, 애플리케이션, 그리고 사용자 서비스를 제공한다. 여기에서 굵은 직사각형은 인터페이스를 나타내며, 굵은 화살표는 의존성을 표시한다. 본 예에서, 디바이스 엔진은 사용자 인터페이스, 디버그 커넥터, 무선 송수신기, RNG, IMEI 등을 포함하는 기본적인 플랫폼 리소스를 제공한다. 디바이스 엔진은 셀룰러 서비스를 제공하는 엔진에게 서비스를 제공하고, 셀룰러 엔진은 애플리케이션 엔진에게 서비스를 제공하며, 또한 애플리케이션 엔진은 사용자에게 서비스를 제공한다.

각 엔진에서 기존의 서비스들은 신뢰 서비스에 액세스하여 각 서비스들의 측정값을 생성하고 이를 모바일 신뢰 모듈(mobile trusted module)에 저장한다. 디바이스, 셀룰러, 애플리케이션 엔진은 MLTM을 갖는데, 이는 각 stakeholder들이 실제로 휴대폰에 액세스하지 않으므로 각 엔진이 요청한 일을 하고 있다는 것을 확인하기 위해 안전한 부트(secure boot) 과정이 필요하기 때문이다. 반면, 사용자는 실제로 휴대폰에 액세스하고 그가 실행하고자 하는 소프트웨어를 로딩할 수 있으므로, 사용자 엔진은 MLTM을 갖는다. MTM은 각 엔진의 현재 상태를 보고하고 이에 대한 증거(evidence)를 제공함으로써 신뢰를 얻을 수 있다. 두 가지 타입의 신뢰 모듈을 갖는 이유는 각기 설계 목적이 다르기 때문이다. MRTM은 IMEI 보호 같은 로컬 검증(local verification)을 구현하는 데 사용할 수 있도록 설계되었고, MLTM은 원격 attestation 같은 원격 검증(remote verification)을 지원하는 데 사용할 수 있도록 설계되었다. 물론 MLTM도 로컬 소유자의 명령 하에서는 로컬 검증 제공에 사용할 수 있다.

(그림 7)은 MRTM이 사용되는 예를 보인 것이다. MRTM은 TPM 1.2 버전의 일부분과 모바일 환경에만 적용되는 새로운 명령어들로 구성된다. RTV와 RTM 모듈은 런타임 환경에서 처음으로 실행 가능한 모듈이다. RTV+RTM 모듈은 측정값을 기록한 후, 제어 권한을 넘기기 전에 MVA를 측정하고



(그림 7) MRTM의 사용 예

검증한다. MVA는 MRTM을 사용하여 실행할 수 있다. MVA는 운영 체제에 제어 권한을 넘기기 전에 운영 체제 이미지를 측정하고 검증한다. 이러한 구조는 안전한 부트를 간략하게 구현한 것이라 볼 수 있다.

MTM 구현을 위해서는 TPM 1.2 버전 중 24개 항목 106개의 명령어들이 필요하며, 이러한 명령어들은 MTRM/MLTM 별로 각각 optional인지 required인지 구분되어 있다. 또한, TPM 1.2 버전 스펙과 다르거나 확장이 필요한 명령어들은 다음과 같다.

- TPM_Extend
- TPM_Init
- TPM_PCRReset
- TPM_ResetLockValue
- Physical Presence
- Localities
- Random Number Generation Requirements
- MakeIdentity and ActivateIdentity
- TPM_FlushSpecific
- Ownership in a MLTM

X. 결론

안전하게 신뢰할 수 있는 플랫폼을 구축하기 위

해 관련 IT 업체들은 기존의 소프트웨어 기반 보안 기능들만으로는 계속되는 보안 패치를 양산해야 하기 때문에 근원적으로 하드웨어 기반 보안 모듈을 컴퓨팅 환경에 적용하고자 산업계 표준화를 진행하고 있다. 본 기고에서는 TCG의 표준화 동향과 차세대 모바일 환경의 신뢰 기반 구축을 위한 동향을 설명하였다. 신뢰 하드웨어를 위한 개방형 TCG 표준은 안전한 PC의 초석을 제공하고 있을 뿐 아니라 향후 차세대 개인 통신 디바이스나 서버에 더욱 견고한 보안 기능들이 제공되도록 할 것이다. 데이터 보호와 플랫폼 무결성 보장이 TCG 스펙의 기본적인 설계 원칙이다. TCG 표준은 특정 운영 체제나 호스트 소프트웨어로 국한되지 않으므로 안전한 플랫폼을 폭넓게 독립적으로 보급할 수 있게끔 한다. 이 기술은 컴퓨팅 실행 환경을 안전하고 신뢰할 수 있도록 하며, 사용자와 기업의 자산을 보호하고 해커들의 유혹을 차단하는 초석이 되어 향후 널리 채택될 것으로 전망한다.

약 어 정 리

BoD	Board of Director
CA	Certificate Authority
CC	Common Criteria
DoS	Denial of Service
EK	Endorsement Key
IMEI	International Mobile Equipment Identity
KCM	Key Cache Manager
MLTM	Mobile Local-owner Trusted Module
MRTM	Mobile Remote-owner Trusted Module
MPWG	Mobile Phone Working Group
MS-CAPI	Microsoft Cryptographic Application Programming Interface
MVA	Measurement and Verification Agent
NFS	Network File System
PCR	Platform Configuration Register
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RTM	Root of Trusted for Measurement
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
SRK	Storage Root Key
TC	Trusted Computing
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TelCo	Tele-conference
TPM	Trusted Platform Module
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System

참 고 문 헌

[1] S. Pearson, “Trusted Computing Platforms: TCPA Technology in Context,” Prentice Hall, 2003.
[2] C. Mitchell, “Trusted Computing,” The Institution of Electrical Engineers, 2005.
[3] S.W. Smith, “Trusted Computing Platforms: Design and Applications,” Springer, 2005.
[4] Trusted Computing Group Website, http://www.trustedcomputinggroup.org