情 報 保 護 學 會 誌
第 16 卷 第 3 號, 2006. 6

모바일 플랫폼용 공통보안핵심 모듈 기술

김 무 섭*, 신 진 아*, 박 영 수*, 전 성 익*

요 약

TCG(Trusted Computing Group)는 더욱 안전한 컴퓨팅 환경의 구현을 목적으로 설립된 업계 컨소시엄으로, 데이터의 신뢰성을 제공하기 위하여 TPM(Trusted Platform Module)으로 불리는 신뢰의 기본을 제공하는 핵심 하드웨어의 사용을 제안하고 있다. 최근 모바일 디바이스의 성능 향상에 따라 다양한 응용들의 지원이 가능해지고, 네트워크를 통한 소프트웨어의 업데이트 및 응용프로그램의 다운로드 등이 가능한 개방형 플랫폼으로의 변화에 따른 디지털 컨버전스는 TMP(Trusted Mobile Platform)라는 새로운 모바일 플랫폼용 규격의 사용을 필요로 하고 있다. 본 고에서는 기존 컴퓨팅 환경과 모바일 플랫폼에 핵심 보안 모듈인 TPM 기술의 국내·외 기술의 동향과 핵심 요소들에 대한 기술적 개념들을 살펴본다.

Ⅰ. 서 론

지난 1999년 Intel, AMD, IBM, HP 및 MS는 end-user의 데이터를 보호하고, 네트워크에서 신뢰성 있는 거래의 확보를 위해 하드웨어를 기반으로 하는 안전한 컴퓨팅 환경 개발을 목표로 TCPA (Trusted Computing Platform Alliance)를 설립하였다. TCPA에서는 TPM (Trusted Platform Module)으로 불리는 하드웨어를 사용하여 컴퓨팅 환경의 신뢰성을 제공하고 사용자 데이터의 안정성을 제공하는 구조를 제안하였다. 최근 컴퓨터 기술의 발전과 개방형 네트워크 기술의 발전에 따라 사용자 컴퓨터의 위협 요인은 더욱 증가하는 추세이며, 더욱 신뢰성 있는 컴퓨팅 환경의 요구에 따라 더욱 많은 컴퓨터 회사와 소프트웨어 회사들이 TCPA의 제안을 수용함으로써 2003년에는 TCG(Trusted Computing Group)로 확대되었다.

TCG에서는 컴퓨터, PDA 및 스마트폰 등의 플랫폼과 플랫폼에서 작동하는 서비스 등이 의도하는 목적에 대하여 예상되는 방법으로 작동 되어질 때 항상 신뢰(trust)할 수 있다고 정의한다. 즉, 플랫폼이 외부의 공격이나 내부의 다른 요인에 의해 변경이나 손상이 되지 않았음을 나타내는 무결성(integrity)을 신뢰의 기본으로 한다. 기존의 플랫폼이나 사용자의 데이터를 보호하기 위해서는 인증(authentication)을 사용하였으나, trusted computing에서는 신뢰의 수단으로 보증(attestation)을 사용한다.

Trusted computing에서 attestation은 플랫폼과 사용자의 데이터를 보호하기 위하여 기존의 인증(authentication)과 플랫폼의 무결성(integrity) 모두를 검증하고, 사용하는 메커니즘이라고 할 수 있다. 따라서 attestation을 위해서는 플랫폼의 구성요소(하드웨어 및 소프트웨어)와 설정 정보 등이 변경되지 않았음을 증명할 수 있는 방법이 필요하다. TCG에서는 이를 위하여 TPM(Trusted Platform Module)의 사용을 제안하였다.

TPM은 물리적으로 tamper-resistant하고 플랫폼에 부착되며, 하드웨어 또는 소프트웨어 공격에 안전한 하드웨어 장치이다. TPM은 암호모듈과 protected storage를 내장하여 플랫폼의 integrity를 측정한 결과를 PCR (Platform Configuration Register)로 불리는 특정 레지스터에 저장하고, 암호모듈과 난수발생기 등을 사용하여 플랫폼의 인증과 신뢰사슬(chain of trust)을 이용하여 integrity를 검

* 한국전자통신연구원 정보보호연구단 무선보안응용연구팀(gomskim, jashin, yspark, sijun@etri.re.kr)
** 본 연구는 정보통신부의 과제로 지원 되었습니다.

증하는 attestation을 수행한다.

TPM을 위해서는 키의 생성과 서명을 수행하는 RSA 공개키 암호모듈, integrity 검증과 인증을 위한 해쉬함수, 사용자 정보와 플랫폼의 attestation 정보를 저장하기 위한 비휘발성 메모리, integrity 정보를 저장하기 위한 별도의 저장장치 및 랜덤 키와 replay attack을 방지하기 위한 난수발생기 등을 기본적으로 내장하여야 한다.

현재까지 trusted computing은 고속의 컴퓨팅 환경을 요구하는 시스템 위주로 개발되었으나, 최근 모바일 컴퓨팅의 수요 증가에 따른 시스템의 안전성이 문제가 되면서 TCG에 모바일 플랫폼 워킹 그룹이 확대 신설되는 등의 움직임을 보이고 있다.

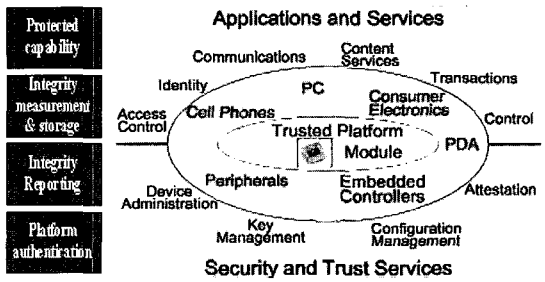
모바일 컴퓨팅 환경도 유·무선 컴퓨팅 환경과 마찬가지로 데이터 및 멀티미디어 서비스가 폭발적으로 증가하고 모바일 인터넷까지 그 영역이 확장되고 있다. 모바일 네트워크가 더욱 복잡하고 많은 어플리케이션의 지원과 컨텐츠의 다운로드 및 m-commerce등의 서비스를 제공함에 따라, 모바일 디바이스도 복잡해지고 가격도 증가하는 추세이다. 또한 모바일 디바이스는 한 개 이상의 라디오 인터페이스를 가지고, 다수의 보안 민감 영역이 인터페이스에 따라서 존재하여, 각 인터페이스는 위험 레벨(integrity 손실 비용 vs. 구현 비용)에 따라 각기 다른 level의 요구사항을 가진다.

또한 차세대 복합 단말기의 경우, 모바일 플랫폼의 시장이 점점 증가함에 따라 도난 및 분실 위험성이 점점 높아지고 있어서 향후 서비스 혹은 고객 불편 신고가 늘어날 전망이며, [표 1]에 나타낸 것과 같이 휴대 단말기의 복제 혹은 ID를 위장하여 이동 통신 및 텔레매틱스 서비스를 불법적으로 이용하거나 프라이버시를 침해하는 가능성이 증가하고 있다.

[표 1] 연간 불법 복제폰 적발건수 및 대수 변동 추이 (자료출처: 정통부)

년도	2000	2001	2002	2003	2004	2005								
						1월	2월	3월	4월	5월	6월	7월	8월	소계
건수	2	2	0	14	43	5	2	26	7	8	8	4	5	65
대수	3	6	0	1,097	858	194	81	983	273	335	1,096	56	1,700	4,718

따라서 지식 정보화 사회의 요구에 부응하고, 고도 산업 기술 사회에서의 신뢰 서비스를 제공하기 위해 기존의 소프트웨어 기반 인증, 암호 알고리즘 및 프로토콜을 다양한 플랫폼에 개별적으로 개발 적용하던 기술에서 탈피하여 하드웨어에 기반하는 공통 보안 핵심 모듈을 개발함으로써 소프트웨어 접근에 의한 보안 한계를 극복할 필요가 있다. 또한 미래의 모바일 플랫폼 환경을 보다 안전하고 신뢰할 수 있는 환경으로 변화시키기 위해 휴대 단말 및 모바일 시스템의 공격을 통한 기밀정보 유출, 위장, 불법 사용, 정상적인 서비스 방해 (DoS공격)를 방지하기 위한 핵심 기술 개발이 요구되고 있다.



[그림 1] TPM의 활용분야 (자료출처: Trusted Computing Group)

모바일 플랫폼용 공통보안 핵심모듈 기술은 [그림 1]와 같이 차세대 이동 통신 환경에서의 인증, 보안 및 신뢰 서비스 제공을 위한 핵심 요소 기술 중에 하나로서, 차세대 이동 단말(예, new DMB, new WiBro 단말), 지능형 모바일 로봇, mobile healthcare 등 IT839정책의 모든 산업 영역에서 신뢰성과 보안성을 제공할 수 있는 핵심 기반 기술이다.

II. Trusted Computing 기술의 동향

1. Trusted Computing 기술의 국제 동향

TCPA는 1999년 컴팩 컴퓨터, HP, Intel 및 마이크로소프트가 결성하여 2001년 신뢰 처리의 isolated computing engine을 정의하고 규격 1.1을 개발하였다. Trusted computing 기술은 개인용 컴퓨터 시스템이 점점 복잡해지고, 특히 랩탑 컴퓨터 및 기타 모바일 장치가 물리적 전자적 공격에 노출될 가능성이 커지고 취약성이 증가함에 따라 그 수요가 점점 더 증가하고 있다.

Trusted computing의 핵심 요소인 TPM은 기본적인 검증뿐 아니라 하드웨어가 변경되지 않고, BIOS가 조작되지 않았으며, 플랫폼이 신뢰할 수 있는 환경에서 구동되고 있음을 검증할 수 있다. 또한 TPM은 다른 컴퓨터와 신뢰성 있는 관계(trusted

relationship)를 구축함으로써 바이러스 및 기타 공격의 기회를 차단할 수 있다. 사용자의 입장에서 trusted computing은 편리하게 한 번에 시스템 sign-on 할 수 있으며, 안전한 트랜잭션을 위한 디지털 서명까지 제공하므로 더욱 신뢰성 있는 통신을 가능하게 해준다.

2003년에는 규격 1.1의 replay attack과 같은 보안 취약성을 해결하고, 위임 기능 및 시스템과 소프트웨어의 정보를 TPM 내부에 저장하기 위한 Non-volatile 저장장치 등을 보강한 TPM 및 TSS 규격 1.2를 발표하였다.

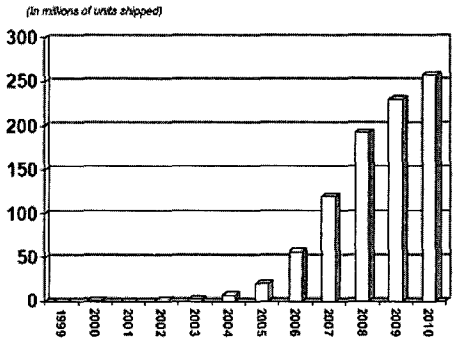
TPM 기술의 개념은 TCG 규격에 기반을 둔 대부분의 신규 컴퓨터 시스템에 채택되고 있다. 현재 개발되고 있는 TPM은 PC 메인보드에 장착되는 형태가 대부분이며 대부분 TPM 규격 1.2를 지원한다. TPM의 주요 개발 업체로는 Atmel, BroadCom, Infineon, Sinosun, STMicroelectronics와 같은 업체들이 있으며, 각 TPM의 특징은 〔표 2〕과 같다.

〔표 2〕 TPM 상용칩 규격 비교(자료출처: ETRI 정보보호연구단)

특징/벤더	Atmel	Infineon	STMicro	Sinosun
모델명	AT97SC3203	SLB 9635 TT 1.2	ST19WP18-TPM-C	SSX35A
암호 엔진	RSA 1024 signature 100ms RSA 2048 signature 500ms		RSA 1024 signature CRT 62 ms, w/o CRT 206ms verification (e=10001) 4ms RSA 2048 signature (CRT) 416ms verification(e=10001) 66ms	RSA 1024 signature <120ms verification <15ms RSA 2048 signature <300ms verification <40ms
마이크로 프로세서	8/16 bit AVR RISC	16bit	8 bit	8 bit
(T)RNG	FIPS 140-2	FIPS 140-2	FIPS 140-2	FIPS 140-2
SHA-1	50 us/64-byte	SHA-1, MD-5		< 258ms/1M bits
키 생성	< 1ms		1.8 s (RSA 1024)	<10 S (RSA 2048)
메모리	ROM(program) E2P(program) E2P(data) SRAM	ROM 64KB E2P 16KB SRAM 8KB	SRAM 2KB	ROM 64KB E2P(program) 128KB E2P(data) 16KB SRAM 16KB
Icc (33MHz)	50 mA (max)			< 30mA

IDC에 따르면, 2005년에 출시되는 컴퓨터 중 2,500만 대가 TPM을 장착하였으며, 2006년에는 약 5,000만 대의 컴퓨터에, 2010년이 되면 거의 대부분의 휴대용 컴퓨터와 데스크톱에 TPM이 내장될 것으로 예상하고 있다(〔그림 2〕 참조).

현재까지 개발된 TPM들이 일부 제품에 장착되어 판매되고 있으며, 점점 TPM을 장착한 제품이 증가하는 추세이다. 대표적으로 세계적인 컴퓨터 메이커인 IBM 이 ThinkPad 노트북과 NetVista 데스크톱, HP의 경우 D530 데스크탑 및 nc시리즈의 노트북에 TPM 칩을 장착하였으며, 2005년부터는 인텔의 Executive 시리즈의 데스크탑 보드 등에 TPM이 장착되고 있다. 그 외 Dell, Fujitsu, Acer 및 Gateway등 다수의 기업 제품에도 TPM의 적용이 증가하고 있다.



〔그림 2〕 TPM 시장 전망 (자료출처: IDC2004)

TPM을 단순히 특정 응용에만 사용하던 기존 방식에 비하여 가장 큰 변화를 주도 할 것으로 예상되는 것은 마이크로소프트이다. 2002년 마이크로소프트는 하드웨어에 기반한 컴퓨터 보안 계획인 NGSCB (Next-Generation Secure Computing Base)를 발표하였으며, 2006년 말에 NGSCB를 적용한 윈도우 비스타 운영체제를 발표할 예정이다.

현재의 윈도우 버전은 파일 폴더와 PC의 암호화를 제공하며, BIOS(Basic Input/Output System) 암호화 같은 기본적인 접근제어 정도의 보안 기능을 제공하고 있다. 그러나 이러한 기능 등은 공격자가 PC에 물리적으로 접근이 가능한 경우 모두 회피할 수 있는 것으로 알려져 있다.

새로 출시될 윈도우 비스타는 인증 받지 않은 사용자들이 PC에 물리적으로 접속해 하드 디스크의 데이터에 접근하는 것을 방지하기 위해 '보안시작' 기능을 포함하고 있으며, 이를 위해 TPM을 사용하여 암호화된 키의 보호된 저장 공간을 제공하도록 하였다.

'보안시작'은 랩탑을 훔치거나 인증을 받지 않은 사람이 컴퓨터에 저장된 데이터를 접근하지 못하도록 설계되었다. 2005년 1월 컴퓨터 보안 연구소(SCI)와 FBI의 보고서에 따르면 미국 기업의 절반이 랩탑 컴퓨터의 도난 경험이 있으며, 피해액은 410만 달러에 달하는 것으로 알려져 있다.

TPM은 암호화된 키, 패스워드 및 디지털 인증서를 저장하는 안전한 저장공간을 제공하며, 윈도우 비스타는 이러한 TPM의 기능들을 사용하여 컴퓨터의 부팅 시 이상이 없다는 점을 확인하고, 암호화를 통해 데이터 보호 및 신뢰성 있는 컴퓨팅 환경을 제공하므로 앞

으로 활용 범위가 점점 더 확대될 것으로 보인다.

2. Trusted computing 기술의 국내 동향

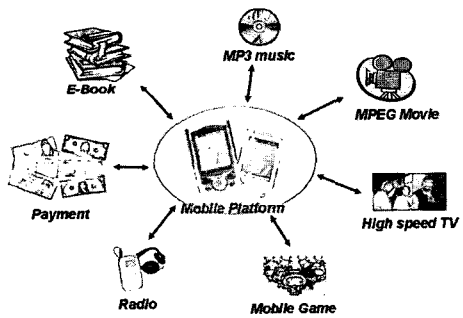
현재까지 국내에서는 삼성전자 시스템 LSI 사업부문에서 스마트카드 기술의 경우 연간 1억개 이상 수출하는 수준이며, 한국전자통신연구원(ETRI)에서 3세대용 USIM 칩 등을 개발하여 기술을 이전한 사례가 있을 뿐, trusted computing 기술에 대해 국내에서는 아직까지 연구가 진행되지는 않고 있다.

국내 업체에서는 삼성전자가 유일하게 TCG에 회원으로 가입하여 활동하고 있으나, 모바일 플랫폼을 위한 공통보안 모듈 기술을 위한 TPM에는 아직 관여를 하지 않고 있으며, 2006년부터 한국전자통신연구원(ETRI)에서 관련 연구를 수행하고 있다.

Ⅲ. Trusted Mobile Platform 기술

TMP(Trusted mobile platform) 기술은 모바일 플랫폼의 integrity을 보장해주는 기술이며, 모바일 기술이 개방형 플랫폼과 가치기반 응용기술로 변화하는 과정에서 새롭게 요구되는 보안사항이다.

최근 모바일 플랫폼은 [그림 3]에서 보이는 것과 같이 기존의 단순한 음성 통신의 기능을 넘어서 모바일 컨버전스가 빠르게 이루어짐에 따라 음악, 사진, 게임, TV, 등의 다양한 기능이 융합된 매우 정교한 기기로 변화하고 있으며, 이에 따라 모바일 플랫폼의 시장 규모는 점점 더 확대되고 있다.

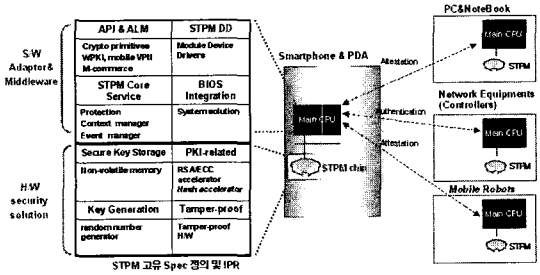


[그림 3] 모바일 플랫폼의 컨버전스(자료출처: ETRI 정보보호연구단)

모바일 플랫폼의 기능이 오픈 플랫폼과 value-based 응용 서비스를 지원하기 위하여 유·무선 인터넷을 통한 소프트웨어 업데이트 및 펌웨어 업그레이드 등으로 기능이 향상되면서, 디지털 컨버전스와 결합한 새로운 해킹 수단이 나타나고 있다. 최근 모바일 스팸의 증가와 같이 해킹의 경로가 유선 인터넷에서 모바일 플랫폼으로 빠르게 확산되고 있으며, Cabir나 Duts 등의 휴대폰 바이러스 역시 2004년 22만 건에 달하는 등, 모바일 플랫폼의 취약성은 점점 더 증가하고 있다.

모바일 플랫폼의 경우 공격에 의해 메모리 내부에 있는 ESN(Electronic Serial Number)이 수정되거나 소프트웨어의 수정에 의해 디바이스의 ID를 유출할 위험이 있다. 또한 디바이스의 하드웨어를 교체하거나 OS를 수정하여 보안 정책을 변경하여 인증되지 않은 프로그램 또는 악의적인 코드를 모바일 플랫폼에 설치 할 수 있다. 플랫폼에 설치된 악의적인 코드는 웜이나 바이러스 등을 이용하여 플랫폼을 파괴 할 수도 있고, 사용자 데이터에 접근하여 사용자의 프라이버시를 위협 할 수 있다.

TMP 기술은 [그림 4]에 나타낸 것과 같이 모바일 플랫폼 장치의 구현을 더욱 견고하게 하고, 플랫폼의 integrity를 유지하며, 플랫폼에 대하여 인가되지 않은 접근 및 수정을 감지할 수 있도록 하드웨어에 기반하는 보안장치인 TPM 칩을 사용하여, 플랫폼의 신뢰성과 보안성을 증가시킨다.

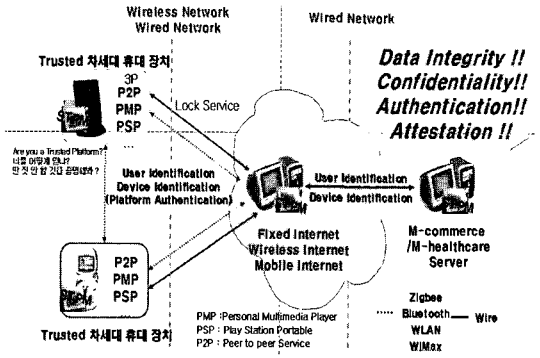


[그림 4] 모바일 플랫폼용 공통보안 모듈의 기술적 개념 (자료출처: ETRI 정보보호연구단)

TMP는 바이러스들과 다른 보안 위협으로부터 디바이스를 안전하게 보호할 수 있도록 설계된 것이며, 이를 통해 모바일 디바이스를 단순히 통화만 하는 장비가 아닌 '전자-티켓'이나 '전자-지갑'과 같은 보다 발전되고 선진화된 애플리케이션에 이용될 수 있도록 한다는 것이다.

TMP기술을 사용한 모바일 디바이스는 [그림 5]와 같이 유·무선으로 다른 디바이스에 연결되어 소프트웨어 업데이트 및 데이터를 다운로드할 수 있으며, 이

러한 과정에서 발생할 수 있는 바이러스나 악의적인 코드의 감염을 방지하여 사용자 데이터를 안전하게 보호하고 신뢰성 있는 컴퓨팅 환경과 네트워크 환경을 제공한다.

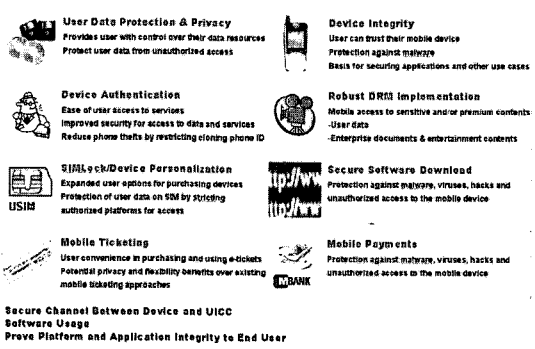


〔그림 5〕 차세대 모바일 환경에서 공통보안모듈 적용 개념 (자료출처: ETRI 정보보호연구단)

모바일 플랫폼용 TPM에 관련한 표준화 활동은 TCG내의 MPWG (Mobile Phone Working Group)에서 수행한다.

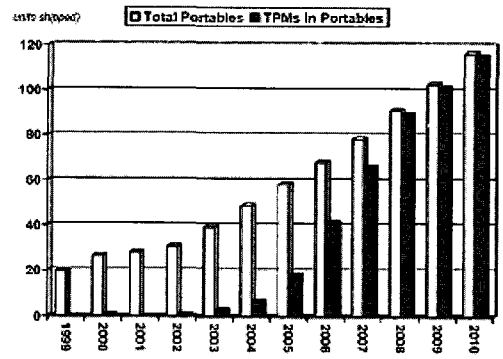
모바일 장비들과 그곳에서 수행되고 있는 소프트웨어와 데이터의 안전을 기하고, 보다 안전한 컴퓨팅 실현을 위해 NTT Docomo, 인텔 그리고 IBM이 공동으로 협력하여 TMP 보안 스펙을 개발, 발표하였다. 이는 하드웨어와 소프트웨어 컴포넌트들, 그리고 테크놀로지 프로토콜들을 포함하는 것을 목표로 하고 있다. 또한, tamper resistant 모듈, 도메인 분할, 그리고 인증과 관리 프로토콜과 같은 보안 기술 및 컨트롤들과도 잘 협동하여 동작하도록 규정하고 있다. IBM, 인텔, 그리고 NTT Docomo는 스펙을 온라인으로 발표했으며, 표준 기관들과 함께 TMP 규격에 대한 리뷰에 착수했다. 메이저 핸드 셋 제공 업체들과 다른 네트워크 오퍼레이터들이 제안을 지지할 것인지, 아닌지의 여부가 아직 남아 있는 상태이다.

MPWG는 모바일 플랫폼을 사용하는 경우에 대해 보안 사항을 정의하고, 향후 모바일 플랫폼의 사용에 대비한 규격을 정의한다. MPWG에서 수행되는 표준화 작업은 먼저, 모바일 플랫폼의 사용 예를 찾고, 각 경우에 대해 요구사항을 정의하며, 해당 요구사항들에 대하여 규격을 정하는 단계로 수행한다. 현재 MPWG에서는 〔그림6〕과 같이 전체 11개의 사용 경우를 분석하여 2005년 9월에 발표를 하였으며, 각 사용 예에 대하여 요구사항을 정의하는 작업을 수행하고 있다.



〔그림 6〕 MPWG의 TMP use cases(자료출처: ETRI 정보보호연구단)

IDC의 전망(〔그림 7〕 참조)에 따르면, 포터블 및 테스크탑에 장착된 TPM의 경우 각각 2006년 4천만 개 및 1천 8백만 개 규모에서 2010년 1억 4천만 개 및 1억 천 5백만 개로 증가 전망이며, 2008년경에 노트북 및 모바일 플랫폼의 90% 이상이 TPM을 적용할 것으로 예상되고 있다.

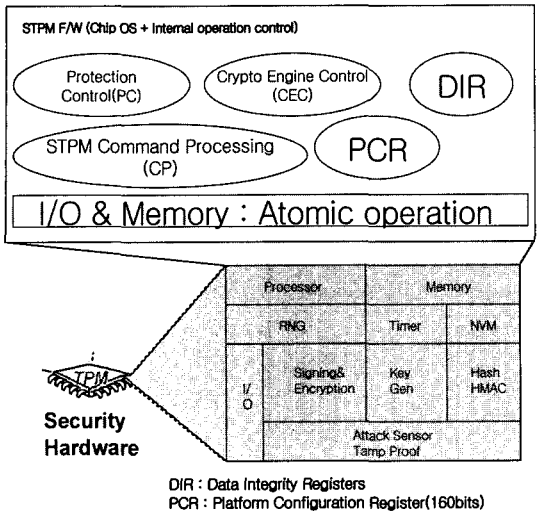


〔그림 7〕 TPM이 장착된 portable 제품의 시장 전망 (자료출처: IDC2004)

TMP 기술은 현재 초기 단계이지만 신뢰 및 보안 관련하여 구현 비용의 감소와 암호 키와 사용자 정보 및 디지털 인증서를 보호해야 하는 필요성이 커짐에 따라 무선 네트워크 보안과 관련해서 사용 추세가 급격히 증가할 것으로 전망된다.

1. Trusted Mobile Platform 구조

〔그림 8〕와 같이 TMP는 모든 명령을 수행하기위해 내부에 프로세서를 사용하고 있으며, 공개키 암호 연산의 고속 처리를 위해 별도의 암호 가속기를 사용



〔그림 8〕 트러스트 모바일 플랫폼의 하드웨어 구조 (자료 출처: ETRI 정보보호연구단)

하고, TMP 또는 사용자의 중요 정보를 유추하기 위한 물리적 공격을 방지하기 위해 tamper resistant 한 장치를 포함하고 있고, 플랫폼의 호스트 프로세서와 안전한 데이터 통신을 수행하도록 설계된 turnkey 방식의 보안 모듈이다.

모바일 플랫폼용 TPM은 내부에서 수행하는 데이터의 보호를 위해 RSA 공개키 암호 알고리즘을 사용하고 있다. 이를 위해 TPM 내부에서 키를 생성하도록 하고 있으며, 연산의 효율성을 고려하여 내부에 키를 저장하는 캐쉬를 사용하여 자주 사용하는 키들을 저장하여 사용하도록 하고 있다. 만일 키가 TPM 외부의 장치에 저장되는 경우, TPM의 내부 키로 반드시 암호화하여 저장하고, 사용하는 경우에는 반드시 TPM을 사용하여 복호화 후에 사용하므로 데이터를 안전하게 저장하고 사용할 수 있다.

TPM이 외부의 공격에 안전하게 동작하고 있음을 검사하고, 검사 결과를 저장하여 모바일 플랫폼의 integrity을 검사하기 위하여 별도의 PCR들을 사용하고 있다.

또한 플랫폼에 대한 replay attack을 방지하고, RSA와 다른 암호 연산을 수행하기 위해 필요한 키를 생성하는 용도로 난수발생기를 사용하며, 데이터의 integrity과 인증 및 PCR 데이터의 확장에 사용하기 위하여 해쉬함수를 필요로 한다.

위의 중요 기능들과 함께 사용자의 개인키와 마스터 키 등의 정보들과 플랫폼의 attestation 정보들을 저장하기 위해 안전한 비휘발성 메모리를 사용하여야 한다. 일반적으로 TMP를 위해서는 다음의 요구사항과 암호기준들을 만족하여야 한다.

1.1 Requirements

TMP를 위해서는 적어도 다음의 사항들을 지원해야 한다.

- TPM 장치의 비밀 정보 및 키를 위해 안전하고 보호되는 저장장치
- 비밀정보의 처리를 위한 안전한 데이터 처리 환경
- 난수 생성을 위한 소스와 키들을 생성할 수 있는 기능
- 디지털 서명의 생성과 검증을 위한 RSA 공개키 암호 기능
- 해쉬함수를 위한 SHA-1 기능
- 명령의 인증을 위해 SHA-1을 이용하는 HMAC
- 안전한 암호기능의 수행과 중간 결과의 변경 및 노출을 방지하기 위한 atomic security operation 기능
- Monotonic 카운터

위의 요구 기능들 외에 TMP는 TCG에서 정의하는 보안 프로토콜들을 추가로 지원해야 하며, 다른 디바이스와의 집적화를 고려하여 설계되는 칩의 크기나 전력소비 등도 고려되어야 한다.

1.2 Cryptographic Engines

TMP 내부에서 중요 데이터와 관련된 연산들이 안전하게 수행되기 위해서는 암호 기능이 제공되어야 한다. 일반적으로 TMP에서는 키의 암호와 서명을 수행하기위한 RSA(PKCS#1 v1.5)와 데이터의 integrity 검증을 위한 SHA-1 해쉬함수(FIPS 180-1)가 반드시 제공되어야 한다. TMP에서 기본적으로 제공해야하는 암호 기능과 특징들을 〔표 3〕에 나타내었다. 그 외 선택사항으로 지원할 수 있는 것으로는 다음의 사항이 있다.

- RSA (PKCS#1 v2.1)
- DH 또는 ECDH 키 일치 알고리즘
- DSA 또는 ECDSA 서명 알고리즘
- DES, 3-DES 또는 AES
- MD5 (RFC 1321)
- SHA-256/384/512

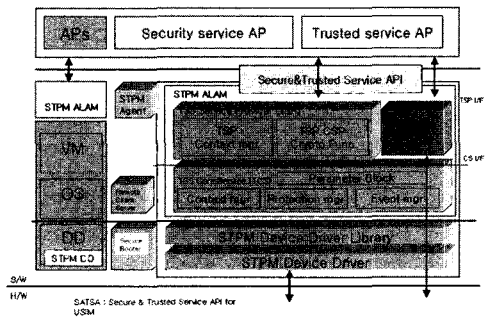
〔표 3〕 Trusted Mobile Platform의 기본 암호 요소 (자료출처: ETRI 정보보호연구단)

Primitives	기능	적용 암호	방법/표준
RNG	- Random seed, output sequence - Hash function	SHA-1, DES	- PRBG: ANSI X9.17, FIPS 186 - CPRBG: RSA, Micali-Schnorr, Blum-Blum-Shub - Output 요구사항: FIPS 140-2
Key generation	- RSA key pairs 생성 - Symmetric key 생성	- RSA	- IEEE P1363 - RNG
Encryption	- Symmetric - Asymmetric	- DES/3DES (TSS support) - RSA	- RSA encryption - DES/3DES encryption (가능시 AES)
Hash function	- Un-keyed - Keyed	- SHA-1 (SHA-256 for AES) - HMAC	- FIPS 180-1, ISO/IEC 10118 - ISO/IEC 9797-2
Digital signature	Asymmetric cryptographic based	- RSA - (DSA, EC-DSA)	- (ISO/IEC 15946-2)
Public key certificates	- 공개키 분배 - data, signature part		- PKCS#1 V2.1 data formatting - X.509 public key certificates

2. Trusted Mobile Platform의 소프트웨어 구조

TMP의 소프트웨어 모듈은 디바이스 드라이버, 디바이스 드라이버 라이브러리, TSS (TCG Software Stack), TCS (TCG Core Services), 및 TSP (TSS Service Providers)로 나뉜다.

일반적으로 디바이스 드라이버를 제외한 소프트웨어 모듈들을 통칭하여 TSS라 하며, 응용 어플리케이션에 TPM 기능의 인터페이스 제공하고 어플리케이션의 실행 및 TPM 구동에 필요한 TPM 자원의 제어 등을 수행한다. 〔그림 9〕은 TMP의 세부 소프트웨어 구성을 나타낸다.



〔그림 9〕 트러스티드 모바일 플랫폼의 소프트웨어 구성도 (자료출처: ETRI 정보보호연구단)

〔그림 9〕의 가장 하위에 위치한 디바이스 드라이버는 TPM 하드웨어 칩으로 명령어를 전달하고, 그에 대한 응답을 TCS로 전달해주는 기능을 하며, 디바이스 드라이버 라이브러리는 TCS와 디바이스 드라이버 사이에서 중간 매개체 역할을 한다.

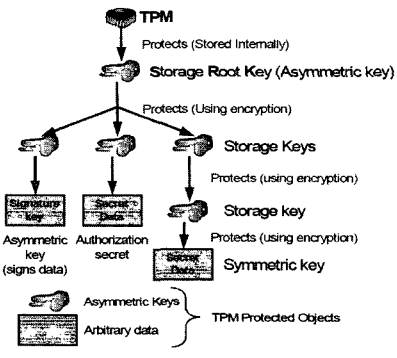
TCS는 어플리케이션 또는 시스템 서비스가 TPM 칩을 사용하고자 할 때, TPM 칩의 제한적인 자원을 효과적으로 관리하기 위해 필요한 키 관리 등과 같은 가장 기본적이고 중요한 핵심 기능을 제공한다. TCS는 Context Manager, Key 및 Credential Manager, Event Manager, 그리고 Parameter Block Generator로 구성되며, 각각의 기능은 TCS 자원의 효율적 관리, 플랫폼과 사용자 프라이버시의 접근제어, PCR의 이벤트 관리, 그리고 TCS로 전달되는 명령어를 byte-stream 형태로 TPM에게 전달하는 것이다.

마지막으로 TSP는 어플리케이션이 TCS 서비스를 사용하기 위한 인터페이스의 제공과 암호 알고리즘 인터페이스 기능을 제공한다. TSP에서 제공하는 암호 서비스는 TPM에서 제공하는 암호기능의 인터페이스를 포함하여야하며, 추가로 산업표준 암호 라이브러리도 제공하여야 한다.

3. Trusted Mobile Platform의 특징

3.1 Protected Capability

TMP는 개인 서명키를 외부에 나타내지 않고 TPM 내부에서 사용하도록 저장할 수 있는 protected storage 기능을 갖는다. TPM 외부에서 사용되는 암호 기능을 위한 암호키나 인증 데이터들은 TPM 내의 protected storage에 저장된 키를 이용하여야만 사용이 가능하다. 이때 사용하는 키들은 〔그림10〕과 같이 TPM 내부에 있는 SRK (Storage Root Key)에 의해 트리 형식으로 TPM이나 외부 저장 장치에 저장되며, TPM 내부에는 키 트리의 root에 해당하는 SRK와 EK(Endorsement Key)만 저장하거나, 사용에서 빠른 접근을 위해 키를 저장할 수 있는 캐쉬를 사용하여 키 트리의 중간 값들을 저장하여 사용하기도 한다.



〔그림 10〕 Protected Storage의 key tree (자료출처: Trusted Computing Group)

TCG에서는 TPM에 사용하는 키로 다음의 7가지 형태의 키를 정의하고 있다.

① Signing 키: 어플리케이션 데이터와 메시지를 서명하는데 사용되는 비대칭키
② Storage 키: 데이터나 다른 키들을 안전하게 저장하는데 사용하는 키로 TCG에서는 RSA 2048 비트의 비도를 가져야 한다고 정의
③ Identity 키: TPM 내부에서만 사용하는 특별한 키로써, TPM 내부에서 생성된 데이터를 서명하는데 주로 사용하므로 attestation 기능을 제공하고, 항상 키 트리에서 SRK 바로 아래에 위치하므로 빠른 접근이 가능하다
④ Bind 키: TPM 외부에서 사용하기 위해 TPM에서 생성하여 전송하는 대칭키와 같이 작은 양의 데이터를 암·복호화 하는데 사용
⑤ Legacy 키: TPM 외부에서 생성하여 TPM 내부로 전송하여 사용할 수 있는 키로써, 데이터 암호와 서명에 동일한 키를 사용하려는 응용에 사용
⑥ Endorsement 키: TPM 내부에서만 사용하는 키 쌍으로써, private 키는 암호 연산이나 서명을 위해서는 절대로 사용해서는 안 되며, 플랫폼에 대해서 복호화 연산만 수행할 때 사용하고, public 키는 TPM 외부에서 공개되어 사용
⑦ Authentication 키: TPM를 포함하여 플랫폼에서 발생하는 데이터 전송 세션들을 보호하기 위하여 사용하는 대칭키

TMP는 모바일 플랫폼의 특정 소프트웨어 환경에서 비밀 데이터를 locking하여 TMP가 해당 환경에서 동작하지 않는 경우에 그 비밀 데이터를 공개하지 않도록 설정할 수 있다.

이러한 기능을 Sealing 이라하며, 특정 소프트웨어의 조건을 활용하기 위해서는 [그림 11]과 같이 TPM 내에 저장된 PCR의 값을 활용한다. 데이터 sealing에 사용하는 키는 TPM 내부에서 키 트리에서 생성한 키를 활용하거나 TPM 외부에서 생성한 키를 사용할 수도 있다.

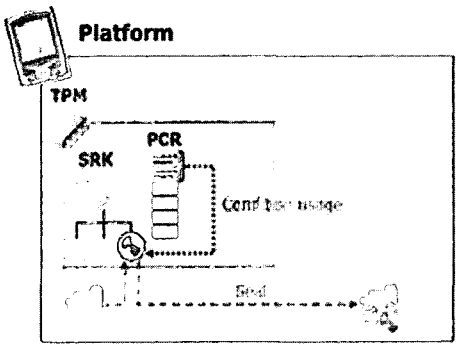
3.2 Integrity measurement와 Reporting

TMP 기술에 적용되는 TPM은 모바일 플랫폼이 부팅되면서 종료될 때까지 모든 연산을 수행하기 전에 플랫폼이 안전하고 신뢰성 있는 환경인지 항상 검사하여야 한다.

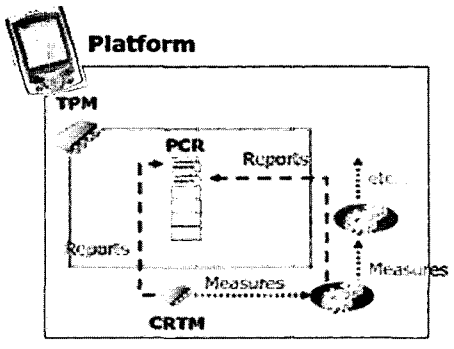
플랫폼이 부팅되면 CRTM(Core Root of Trust for Measurement)라고 불리는 장치로부터 BIOS와 다른 펌웨어 및 소프트웨어의 integrity를 측정하여 그 값을 TPM의 PCR에 저장한다. 이때 integrity 측정이 되는 프로그램들은 내부에 integrity를 측정할 수 있는 일련의 명령들을 포함하고 있어서, 다음에 수행되는 프로그램들의 integrity를 계속해서 측정한다. 일단 OS가 성공적으로 로드될 때까지 이러한 측정은 계속 수행되며, 측정된 값들은 계속해서 TPM내의 PCR에 저장된다.

OS가 성공적으로 load되면, OS에 포함된 measurement agent가 이후에 load되는 소프트웨어의 integrity를 측정하고 다시 PCR에 저장한다.

즉, TPM의 integrity 측정은 이전에 실행되는 컴포넌트가 다음 컴포넌트의 integrity를 측정하는 과정의 연속으로 볼 수 있다. 이러한 과정에서 측정된 데이터는 measured data와 measurement digest



[그림 11] TMP의 데이터 sealing 개념 (자료출처: Trusted Computing Group)



[그림 12] TPM에서 integrity 측정 (자료출처: Trusted Computing Group)

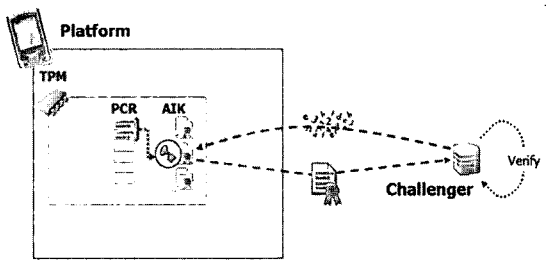
로 분류된다.

Measured data는 측정되는 소프트웨어의 이름이나, 제작사명, 버젼 정보 등의 데이터로써, 측정된 값들이 순서대로 저장되는 공간인 SML(Stored Measurement Log)에 저장된다. Measured data는 TPM 외부의 저장 공간에 저장되며, 반드시 안전하게 저장될 필요는 없다.

Measurement digest는 measured data를 해쉬 함수를 이용하여 처리한 값으로써, TPM 내부의 PCR에 저장되어 불법적인 변경이 불가능하다.

Integrity를 측정한 값이 저장되는 PCR은 일반적으로 SHA-1 해쉬 함수를 수행했을 때의 결과 값인 160 비트의 크기를 가지며, 새로운 값을 측정하면 이전 값이 저장된 PCR에 새로 측정된 값을 연접한 후, 이 값을 다시 해쉬 연산을 수행하여 항상 일정한 크기를 갖도록 하고 있다. 이러한 방식의 사용은 하나의 PCR로 많은 측정값들을 저장할 수 있다는 장점이 있다. TCG는 TMP 기술에 사용되는 TPM에는 사용 목적에 따라 다르지만 보통 8개의 PCR을 사용하도록 규정하고 있다.

플랫폼의 integrity 검증을 위해서는 Integrity reporting 과정을 수행하는데, 보통 [그림 13]에서와 같이 challenge- response 방식을 사용한다.



[그림 13] TMP의 integrity 검증 (자료출처: Trusted Computing Group)

Integrity의 검증을 원하는 challenger는 TPM에 nonce를 전송한다. TPM은 challenger가 보낸 nonce에 PCR 값을 같이 서명을 하고, SML에 저장된 log값과 서명의 검증에 필요한 인증서를 challenger에게 전송한다. Challenger는 전송되어 온 인증서를 이용하여 TPM의 서명으로부터 nonce와 PCR값을 복원하고, log값들을 이용하여 해쉬 연산을 수행하여 PCR 값과의 일치 여부를 검사함으로써 플랫폼의 integrity를 검증한다.

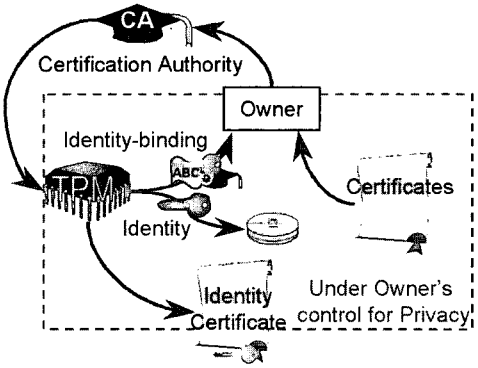
3.3 Platform Identification과 Certification

모바일 플랫폼의 identity는 해당 플랫폼이 TCG의 규격을 만족하는 하드웨어 및 소프트웨어로 구성되어 있음을 이미 검증 받았음을 나타내는 것으로 정의되며, 하나의 플랫폼은 여러 개의 identity를 가질 수 있다.

플랫폼의 identification을 위해서는 플랫폼의 인증과 플랫폼의 환경을 attestation 할 수 있는 키가 필요하다. TCG의 규격에 의하면, EK (Endorsement Key)는 TPM 내부에서만 사용해야하고, 암호 연산이나 서명을 위해서는 사용할 수 없도록 규정하고 있다. 따라서 모바일 플랫폼의 확인을 위해 AIK (Attestation identity Key)를 사용한다. AIK는 서명키로써 사용되며, AIK를 생성한 플랫폼에서만 사용이 가능하다.

모바일 플랫폼의 identity를 위해 EK는 플랫폼의 AIK들을 attestation하는데 사용하고, 플랫폼의 확인은 AIK를 사용함으로써, 플랫폼은 다른 identity를 갖더라도 항상 동일한 플랫폼임을 EK가 보장하도록 하고 있다.

플랫폼의 identity를 위해서는 EK와 AIK 외에 플랫폼이 TCG에서 규정하는 대로 안전하게 설계 및 제작되었음을 증명하는 자료가 필요하다. 모바일 플랫폼에서는 플랫폼 내의 TPM과 TPM이 TCG 규격에 따라 적절하게 설계되었음을 나타내는 증명서(TPM Endorsement Certificate)와 플랫폼이 TPM을 안전하고 규격에 맞게 설치하였음을 나타내는 증명서(Platform Certificate) 및 플랫폼의 ID가 플랫폼 내의 TPM에서 발급되었음을 증명하는 증명서(Platform Identity Certificate) 등이 사용된다.



[그림 14] TPM의 identity 생성 (자료출처: Trusted Computing Group)

모바일 플랫폼의 ID 생성의 간략한 절차를 [그림 14]에 나타내었다. 플랫폼의 소유자가 새로운 ID의 생성을 원하면, TPM은 새로운 공개키 쌍을 생성한다. TPM은 새로 생성한 공개키 쌍의 public key와 TPM 소유자가 선택한 이름, TPM 소유자가 선택한 CA(Certification Authority)의 정보들을 새로 생성한 공개키 쌍의 private key로 서명한 identity-binding을 생성한다.

플랫폼은 CA에게 identity-binding 값과 플랫폼이 신뢰할 수 있음을 나타내는 증명서들 (endorsement, platform credential)을 취합하여 CA의 public key로 암호화하여 전송한다.

CA는 전송된 증명서들과 identity-binding을 검사하여 새로운 ID이면, 해당 ID에 대한 attestation certificate을 생성하고 세션 키를 사용하여 암호화하여 TPM으로 전송한다. CA는 certificate을 암호화하는데 사용한 세션 키와 identity-binding에서 얻은 public key를 암호화한 해쉬 값을 TPM의 public endorsement key를 이용하여 암호화하여 TPM에게 전송한다.

TPM은 identity key에 대한 해쉬의 복호화 값을 검사하여 동일하면, CA로부터 세션 키를 복원하여 identity certificate을 얻는다.

이러한 과정들은 TPM 내부의 암호 연산과 키 값들을 이용하여 진행되므로, 외부의 공격에 의해 플랫폼의 ID는 도용 될 수 없으며, 모든 핵심 연산을 하드웨어를 기반으로 하는 TPM이 수행함으로 가능하다.

Ⅳ. 결 론

본 논문에서는 안전한 컴퓨팅 환경의 구축을 목표로 최근 해외에서 활발한 연구를 수행하고 있는 trusted computing 기술과 관련 기술의 국내·외 동향을 살펴보았다. 최근 모바일 플랫폼은 디지털 컨버전스가 빠르게 이루어짐에 따라 음악, 사진, 게임, TV 등의 다양한 기능이 모바일 플랫폼으로 융합되고 있으며, 이에 따라 모바일 플랫폼에 대한 보안위협도 증가하고 있다. 이에 대한 방안으로써 trusted computing의 핵심 기술인 TPM을 모바일 플랫폼에 적용하는 TMP 기술을 살펴보았다.

모바일 플랫폼용 공통보안 모듈 기술은 기존 trusted computing 기술에 비해 소비전력과 칩 면적 등 플랫폼에서 사용할 수 있는 자원의 제약 때문에 개발에 어려움이 있으나, 아직 기술 개발의 초기에 있으며, 표준화 역시 진행 단계에 있다.

따라서 적절한 시장의 예측과 모바일 플랫폼용 핵심 보안 모듈의 개발은 현재 우리 나라가 선점하고 있는 정보통신 강국의 위상을 유지하고 확장하는데 있어 반드시 필요한 기술이라 할 수 있을 것이다.

참 고 문 헌

[1] Siani Pearson, "Trusted Computing Platforms: TCPA Technology in Context", *Prentice Hall*, 2003.

[2] 전성익 외, "STPM개발 Workshop 자료집", ETRI 무선보안응용연구팀, 2006.

[3] R.Sailer 외, "Design and Implementation of a TCG-Based Integrity Measurement Architecture," *IBM Research Report*, 2004.

[4] Ross Anderson, *'Trusted Computing' Frequently asked Questions*, 2003, http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html

[5] Trusted Computing Group, *TCG TPM Specification Version 1.2*, 2004, http://www.trustedcomputinggroup.org/downloads/specifications/mainP1DP_rev85.pdf

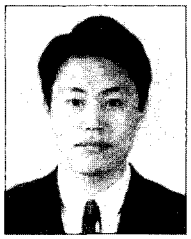
[6] Trusted Computing Group, *Trusted Computing Group Specification Architectural Overview, Revision 1.2*, http://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf

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

[8] Reiner Sailer외, Design and Implementation of a TCG-based Integrity Measurement Architecture, *13th Usenix Security Symposium*, 2004.

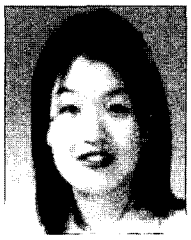
[9] Richard Stallman, Can you trust your computer?, 2002. http://www.gnu.org/philosophy/can-you-trust.html

〈著 者 紹 介〉



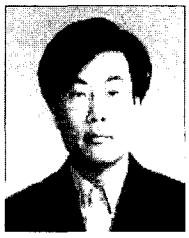
김 무 섭 (Moo-seop Kim)
정회원

1995년 2월 : 금오공과대학교 전자공학과 졸업
1998년 2월 : 경북대학교 전자공학과 석사
1998년 2월~1999년 8월 : LG종합기술원 Innovation Center 연구원
1999년 9월 ~ 현재 : 한국전자통신연구원 무선보안응용연구팀 선임연구원
관심분야 : 정보보호 및 응용, 암호회로 설계



신 진 아 (Jin-a Shin)
정회원

2000년 2월 : 한동대학교 전산전자공학부 졸업
2002년 2월 : 한국정보통신대학교 정보공학부 석사
2002년 3월~현재 : 한국전자통신연구원 무선보안응용연구팀 연구원
관심분야 : 모바일 플랫폼 보안, 스마트카드



박 영 수 (Young-Soo Park)
정회원

1985년 2월 : 중앙대학교 전자공학과 졸업
1987년 2월 : 중앙대학교 전자공학과 석사
1990년 ~현재 : 한국전자통신연구원 무선보안응용연구팀 책임연구원
관심분야 : 저전력회로 설계, 암호프로세서 설계

전 성 익 (Sung-ik Jun)
정회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
1987년 3월~현재 : 한국전자통신연구원 무선보안응용연구팀 팀장
관심분야 : 스마트카드 구조 및 OS, 무선보안, 플랫폼보안