Trusted Computing 기술 및 TCG 표준화 동향

Trusted Computing Technology and TCG Standard Trend

21세기를 대비하는 정보보호 특집

박정숙 (J.S. Park) 무선보안응용연구팀 선임연구원
조태남 (T.N. Cho) 우석대학교 정보보안학과 조교수
한진희 (J.H. Han) 무선보안응용연구팀 선임연구원
전성익 (S.I. Jun) 무선보안응용연구팀 팀장

목 차

인터넷을 제공하는 컴퓨팅 환경에서는 점점 더 다양한 해킹 공격이 늘어가고 있으며 이를 방지하기 위한 운영체제나 소프트웨어의 끊임없는 보안 패치는 필수요소로 여겨지고 있다. 이에 따라 이러한 문제를 근본적으로 해결하려는 시도가 생겨나게 되었고, 그 결과 TC 기술이 연구·개발되었다. TC 기술이란 컴퓨터가 당초 의도된 대로 동작할 수 있도록 신뢰성을 부과하는 기술로서, 하드웨어 기반의 보안칩인 TPM을 모든 컴퓨팅 파워가 있는 기기들에 공통으로 적용하도록 하고, 이를 위한 소프트웨어를 개방형 표준으로 제공하고자 하는 기술이다. 이 기술은 매우 다양한 활용영역을 가지고 널리 사용될 수 있을 것으로 기대된다. 본 고에서는 TC 기술 요소들의 특징 및 기술 동향을 살펴보고, 1999년부터 TCG를 중심으로 진행되고 있는 TC 표준 동향과 쟁점사항들, 향후 TC 기술 및 활용 전망에 대해 기술한다.

Ⅰ. 서론

TC 기술이란 컴퓨터가 당초 의도된 대로 동작할 수 있도록 신뢰성을 부과하는 기술로서, 하드웨어 기반의 보안칩(security chip)인 TPM을 모든 컴퓨팅 파워가 있는 기기들에 공통으로 적용하도록 하고, 이를 위한 소프트웨어를 개방형 표준으로 제공하고자 하는 기술이다[1]-[3].

현재 인터넷 환경을 제공하는 컴퓨팅 환경은 다양한 해킹 공격이 양산되고 있으며 끊임없는 보안 패치를 수행해야 하는 상황이다. 이에 따라 이를 근본적으로 완화하는 기술이 필요하게 되었는데, 그 한 예로 TC 기술은 기존의 컴퓨터와 차별화된 신뢰할 수 있는 최소 모듈을 플랫폼에 고정형으로 내장하여 원하면 플랫폼의 현재 상태를 로컬 혹은 원격에서 검증할 수 있도록 하기 위하여 등장하였다. 이는 2002년부터 기술 개발을 시작하여 2004년 PC 및 노트북 PC에서는 괄목할 만한 결과를 만들어 냈다.

앞서 기술한 것처럼 의도된 대로만 작동하는 플랫폼을 신뢰 컴퓨팅이라 한다. 예를 들어 e-mail을 송·수신할 때, e-mail의 송·수신 기능 이외의 PC 변화가 일어난다면 의도된 것과 다르게 작동하는 것이다. 현재는 사용자가 이를 인식할 수 없지만 TC 기술을 채용하면 이러한 상황을 인식할 수 있게 된다. 즉, TC 기술은 어떤 응용 프로그램이나 상대 플랫폼이 알 수 없는 콘텐츠에 접근하고자 한다든지, 권한 범위를 벗어나서 플랫폼에 읽기 혹은 쓰기 접근을 시도할 때 즉시 이를 사용자에게 알려주도록 한다[1]-[4].

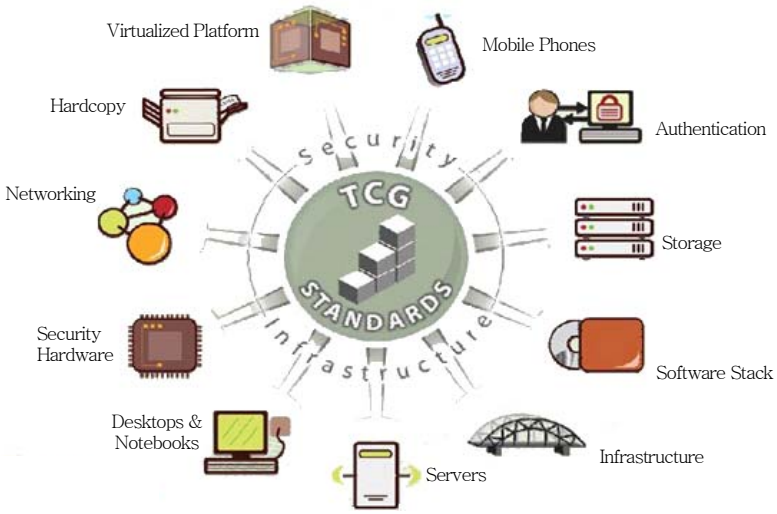
TC 기술은 TPM과 TSS 및 분야별 응용 펌웨어(firmware) 혹은 소프트웨어 라이브러리(software library)로 구성되어 사용자 및 제조사 모두에게 신뢰 기반을 제공한다. TC 기술은 (그림 1)에서 보는 바와 같이 컴퓨터 인증, 네트워크, 프린팅, 이동전화, 응용 프로그램 보안에 널리 사용될 수 있다.

Ⅱ장에서는 TPM 기능, TPM을 채용할 때 새롭게 제안된 핵심기술, TPM 적용 사례 및 특징을 기술하고, Ⅲ장에서는 TCG의 표준화 동향을 소개하며, Ⅳ장에서 결론을 맺는다.

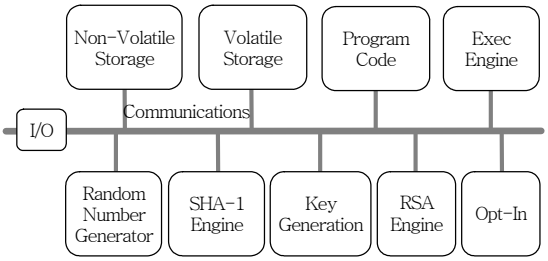
Ⅱ. TC 기술 동향

1. TPM 구조

TC 기술의 핵심 구성 요소인 TPM은 tamper proof circuit으로서 (그림 2)와 같이 구성되며, 각 구성 요소의 역할은 다음과 같다[1],[5],[6].



(그림 1) TC 기술 활용 분야



(그림 2) TPM 구조

- Non-Volatile Storage: 비휘발성 저장소로서, SRK와 EK가 저장된다.
  - SRK: 스토리지 보안 체인의 시작점이 되는 키로서 TPM 외부에 저장된 키들을 보호하기 위한 최상위 키이다.
  - EK: TPM을 식별하고 인증하는 키로서 각 TPM 고유의 유일한 키이다.
- Volatile Storage: 휘발성 저장소로서 PCR들과 AIK가 저장된다.
  - PCR: 8~24개로 구성되며, 컴퓨터의 상태 정보를 저장한다.
  - AIK: 데이터에 대한 디지털 서명키이며, 여러 개를 생성하여 저장 및 사용할 수 있다.
- Program Code: TPM에 내장되는 코드를 저장한다.
- Random Number Generator: NIST SP 800-22 표준을 따르며 Triple-DES와 AES 키로 사용하기 위한 128비트 혹은 256비트 난수를 생성한다. 또한 key generation 모듈에서 RSA 키 생성에 필요한 seed를 생성하여 제공한다.
- SHA-1: FIPS 180-1 표준을 따르며, 160비트 해시 값을 생성한다.
- Key Generation: IEEE P1363 표준을 준수하며, 2048비트 RSA 키 쌍을 생성한다.

● 용 어 해 설 ●

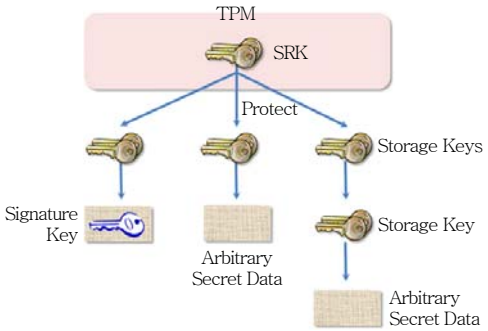
PCR(Platform Configuration Register): 플랫폼의 상태 값을 저장하기 위해 존재하는 160비트 레지스터로 TPM 버전에 따라 8~24개까지 존재한다. PCR에 저장된 값은 플랫폼이나 소프트웨어의 무결성을 검증하는 데 사용된다.

- RSA Engine: IEEE P1363 표준을 준수하여 2048비트 키를 사용한 RSA 암·복호를 수행한다.
- Opt-In: TPM 칩의 특정 기능 접근 권한, NV enable/disable flags 및 ownership을 관리한다.
- Exec Engine: 칩 운영체제와 TPM 명령어를 처리한다.

2. TPM 특징

가. Protected Storage 및 Shielded Locations

TPM은 개념적으로 무제한의 protected storage를 제공하는 포털의 역할을 한다. 즉, 외부의 어떠한 공격으로부터 데이터, 키, 인증서 등을 안전하게 보호할 수 있는 저장 영역을 제공하고 있으며, 특히 키 저장 및 관리 부분에 초점을 두고 있다. 일례로, 비밀 키를 TPM 칩 외부로 유출하지 않으면서 암·복호 및 서명 검증 기능을 수행하도록 설계되었다. (그림 3)에서와 같이 TPM은 SRK를 가지고 storage key들을 암호화한다. Storage key들은 비밀 정보를 암호화하거나 또 다른 storage key들을 암호화하기 위해 사용되기 때문에 (그림 3)과 같이 트리 형태의 계층 구조를 이루게 된다. TPM이 보호하는 비밀 정보는 데이터나 메시지의 암·복호화에 사용되는 대칭키나 디지털 서명에 필요한 서명키 등이 될 수 있다. SRK와 storage key들은 모두 비대칭키를 사용하며, TPM의 제한된 저장공간 때문에



(그림 3) 스토리지 계층 구조

SRK만 TPM 내에 저장하고 나머지는 TPM 외부에 저장한다. 비밀 정보에 대한 요청이 있으면, TPM은 SRK로부터 요청된 비밀 정보까지의 경로상에서 parent key로 child key를 차례로 복호화하는 과정을 반복하고 마지막으로 복호화된 단말 값이 요구되는 비밀 정보이므로 이를 반환한다.

TPM의 중요한 기능 중의 하나는 비밀 정보에 대한 봉인(seal) 기능이다. 이것은 소프트웨어가 요구되는 특정 상태에 있을 때만 저장된 비밀정보를 반환할 수 있도록 하는 기능이다. 이를 위해 TPM은 비밀 정보를 저장할 때 반환시 만족해야 하는 상태값(PCR)을 생성하여 비밀 정보와 함께 저장하고, 반환 요구시 현재의 상태가 저장된 PCR 값이 일치할 때에만 비밀 정보를 반환한다[1].

나. Cryptographic Capabilities

스마트 카드나 보안 토큰과 마찬가지로 암호 알고리듬 및 알고리듬에 사용되는 키에 대한 정보를 저장하고 처리하는 기능을 담당하며, 암호 가속을 위한 수단을 갖추고 있다. 지금까지 제정된 표준에 따르면 비대칭키 암호(2048bit RSA), 키 생성(RSA 키 쌍 생성 내장, 대칭키 생성), 해시(SHA-1, SHA-256), RSA 서명, TRNG 난수 생성 등이 언급되고 있으며 향후 ECC-384, AES-256을 선택 적용할 수 있는 표준이 제시될 예정이다.

다. Protected Execution

TPM은 플랫폼의 신뢰성을 설정하는 근간이 되는 RoT를 네 가지 종류로 제공하고 있다. 이는 플랫폼을 왜곡시킬 수 있는 외부 공격으로부터 플랫폼 무결성을 보장할 수 있는 방법으로 활용될 수 있다. TPM 내에 믿을 수 있는 단서(일명 RoT)는 RTS, RTM, RTR, RTV 등으로 제공된다. 이는 소프트웨어 공격으로부터 보호되며 물리적인 해킹방지 기능으로 보호된다. 예를 들어 RTM을 이용하여 TPM이 장착된 플랫폼에서 수행되는 모든 소프트웨어의 무결성을 검증하여 믿을 수 있는 소프트웨어만이 수행되도록 함으로써 플랫폼의 신뢰성을 지원한다. 또한 플랫폼이 부팅되는 과정에서도 무결성을 검증하여 신뢰성 있는 환경을 제공한다. 이를 지원하기 위해서는 기존 운영체제의 수정이 요구되는데 이 기능을 제공하는 처리 절차는 5절에서 기술한다.

라. Remote Attestation(원격 검증)

TPM이 장착된 플랫폼에서는 통신하고자 하는 플랫폼이 신뢰할 수 있는 상태인지 원격으로 검증할 수 있다. TPM은 TPM만의 유일한 키인 EK를 보유한다. 그러나 이 키를 자신을 검증하기 위해 빈번하게 사용한다면 노출의 위험성이 커질 뿐 아니라 TPM의 익명성을 지원할 수 없게 된다. 따라서 TPM의 익명성을 지원하면서도 자신이 믿을 수 있는 플랫폼임을 증명하기 위해 AIK를 별도로 생성하여 사용한다. 하나의 TPM은 여러 개의 AIK를 가질 수 있으며 자신을 검증하려고 하는 상대방(verifier)에 따라 다르게 생성하여 사용할 수 있다. AIK는 Privacy-CA로부터 인증받거나 DAA 기술을 통해 신뢰할 수 있는 TPM이 생성한 키임을 상대방에게 입증해야 한다. TPM은 현재 플랫폼의 상태를 나타내는 여러 가지 PCR 값을 생성하여 저장하고 있기 때문에 자신이 신뢰할 수 있는 상태임을 증명하기 위해 AIK로 서명된 PCR 값을 상대방에게 전송하고, 상대방은 이 PCR 값을 확인함으로써 플랫폼이 신뢰할 수 있는 상태임을 검증한다. 자세한 검증 절차는 7절에서 기술한다.

3. TPM PCR

TPM 내에는 플랫폼의 상태 값을 저장하기 위한 160비트 레지스터인 PCR이 8개~24개 존재한다. PCR은 외부에서 직접 쓰기가 불가능하고 정해진 절차와 인터페이스를 통해서만 값을 extend 할 수 있다. TPM은 PCR 값을 기반으로 플랫폼이나 소프트웨어의 무결성을 검증하고, 봉인된 비밀 정보가 특정 조건에 맞을 경우에만 반환될 수 있도록 하는 기능을 제공한다.

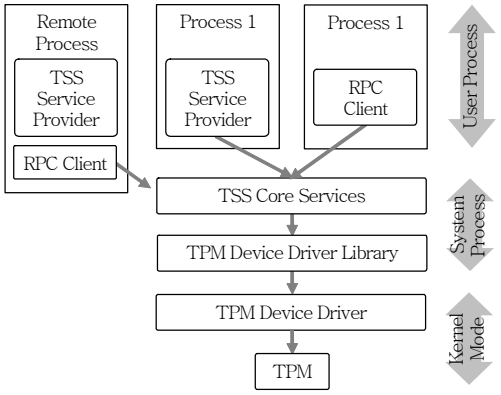
새로운 PCR 값은 아래 식과 같이 기존의 PCR 값에 추가되는 값을 접합(concatenate)한 다음 SHA-1 알고리듬을 이용하여 얻어진다. 따라서 PCR은 일정 길이로 유지되며, 업데이트된 시점까지 누적된 무결성 검증 결과를 저장하게 된다[1],[7].

$$PCR_{new} = SHA\text{-}1(PCR_{old} \| \text{Extended value})$$

4. TSS 기술

TSS 기술은 TPM을 채용하고 신뢰서비스를 응용 서비스로 쉽게 구축할 수 있도록 해주는 미들웨어로서, (그림 4)와 같이 TSP, TCS, TDDL 및 TPM Device Driver로 구성된다. 각 구성 요소의 기능은 다음과 같다[8].

- TSP: 애플리케이션들이 TCG 기능을 사용하기 위한 인터페이스를 제공한다. 애플리케이션마다 독립적인 TSP 인스턴스를 생성하여 사용할 수 있다.
- TCS: TSP는 TPM과 바로 통신할 수 없고, TCS를 통해서만 가능하다. TSP에서 공통으로 필요한 기능을 공유할 수 있도록 관련 기능들을 제공해 준다.
- TDDL: TCS와 Device Driver 사이의 중간 모듈이다.
- TPM Device Driver: TPM에 명령어를 전달하고 처리 결과를 받아서 TDDL에 전달하는 역할을 담당한다. TPM 종류와 OS에 의존한다.

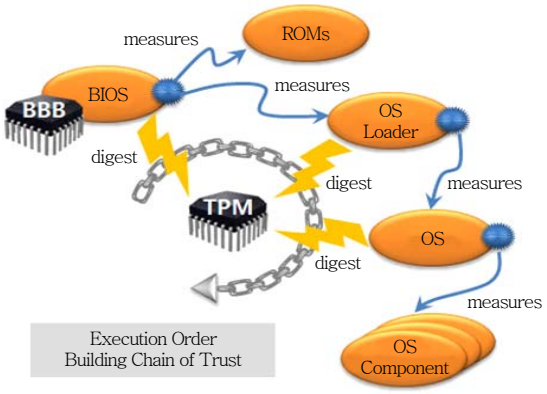


(그림 4) TSS 구조

5. IMVA 기술

TPM이 장착된 플랫폼에서는 수행되는 소프트웨어가 신뢰할 수 있는지를 검사하기 위해 measurement agent가 상주하면서 소프트웨어의 무결성을 검증하고 기록한다. 또한 플랫폼이 부팅된 후 measurement agent가 상주하기까지의 과정에 대해서도 무결성을 검증함으로써 신뢰성을 확보한다. (그림 5)에서 보는 바와 같이 BBB가 BIOS를 실행시키면 BIOS 내에 존재하는 measurement agent는 다음 수행 블록인 OS loader와 ROM에 대한 무결성을 측정하고 측정치에 대한 결과 값을 TPM 내의 PCR에 저장한 후, 다음 수행 블록인 OS loader로 제어권을 넘긴다. OS loader 내의 measurement agent는 동일한 방법으로 OS의 무결성을 측정하고 결과 값을 PCR에 저장한 후, OS로 제어권을 넘김으로써 신뢰성 있는 부팅이 완료된다. 로딩된 OS는 이후에 수행되는 모든 블록에 대하여 무결성을 측정함으로써 부팅부터 소프트웨어 실행까지의 신뢰체인이 이와 같은 단계를 거쳐 형성된다[1],[4].

이 과정에서 생성되는 무결성 측정 결과는 TPM 외부 저장소에 measurement log로 저장되는데 이 값들은 추후 PCR 값을 이용한 무결성 검증과정에 사용된다.



(그림 5) 신뢰 체인

6. Device/Platform 인증 기술

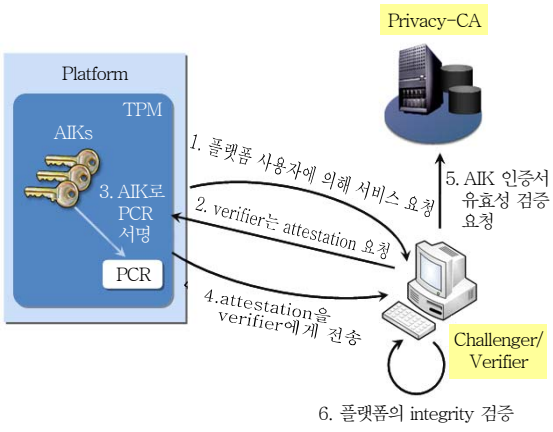
Device/Platform에 부착된 TPM은 고유한 ID를

저장하고 있으며 이를 검증할 수 있는 기능을 제공한다. 또한, ID 개념에서 나아가 하드웨어 제조사, 플랫폼 제조사 등의 인증서 정보를 TPM 내에 저장하고 있기 때문에 필요시 이를 검증하여 인증을 수행한다. 이는 공개키 기반 사용자 인증과 개념적으로 동일하지만 기기 인증서 기반 인증이 가능하다는 의미이다. 즉, 세심한 인증을 고려하는 경우에 대비하여 플랫폼의 ID 뿐만 아니라 무결성 정보까지도 인증 범위에 넣어서 사용할 수 있도록 제공한다. 이는 TPM 채용 기기 및 platform을 사용하기에 앞서 platform의 시작 시점 초기 환경(소프트웨어, 하드웨어, configuration 정보 등)을 PCR에 저장하여 새로운 소프트웨어가 설치 혹은 변경될 때마다 PCR을 extend하여 무결성 체크도 동시에 가능하게 한다는 의미이다.

플랫폼 인증이란 플랫폼의 고유 번호와 플랫폼이 의도한 대로 무결성이 보장되고 있는지를 검증하는 것으로 검증 결과에 따라 보안 정책을 원격 혹은 로컬로 수립 시행 가능한 특징이 있다.

7. Attestation 기술

TPM이 장착된 플랫폼들은 통신 대상이 안전한 상태인지 검증할 수 있다. (그림 6)에서와 같이 어떤 플랫폼의 사용자가 서비스를 요청하면, verifier는 서비스를 요청한 플랫폼이 안전한 상태인지를 검증하기 위해 nonce 값과 함께 attestation 요구 메시지를 전송한다. 플랫폼은 수신한 nonce와 현재의 상태를 나타내는 measurement log와 이에 대한 PCR 값을 안전하게 보호하여 verifier에게 전송한다. 이 값은 verifier에 대응되는 AIK로 서명하여 보냄으로써 무결성이 보장된다. PCR 값을 수신한 verifier는 자신이 보낸 nonce를 확인하고 Privacy-CA로부터 AIK가 신뢰할 수 있는 플랫폼의 키임을 검증한다. 또한 AIK로 서명한 PCR 값의 무결성을 검증하고, 이 PCR 값은 measurement log에 대한 해시 값임을 검증함으로써 신뢰할 수 있는 플랫폼임을 확인한다.



(그림 6) 원격 검증 절차

8. Advanced TPM 기술

TPM1.2 이후에 제안되어 TPM.Next까지 계속 언급되고 있는 추가 기술들은 다음과 같다.

- Key Migration and Certified Migratable Keys
- DAA
- Monotonic Counters and Time Stamping
- NV Storage Management
- Maintenance
- Transport Sessions
- Delegation
- Locality for Virtualization

9. TC의 단점 극복

Linux는 개방형 표준 형태로 불특정 다수에게 공개하여 소프트웨어를 자유롭게 개발하게 함으로써 소프트웨어 생산성 향상을 기대할 수 있는데 반해, TC에서는 이를 엄격하게 제어함으로써 소프트웨어 산업 발전을 저해하는 요인이 존재하고 있으며, 모든 기기들이 동일한 TPM을 기본적으로 장착하여야 TC의 실효성이 있다는 한계점을 가지고 있다. TC가 보편화되어 상용화될 시점이 언제 올지는 미지수로 남겨진 상태이다.

Ⅲ. TCG 표준화 동향

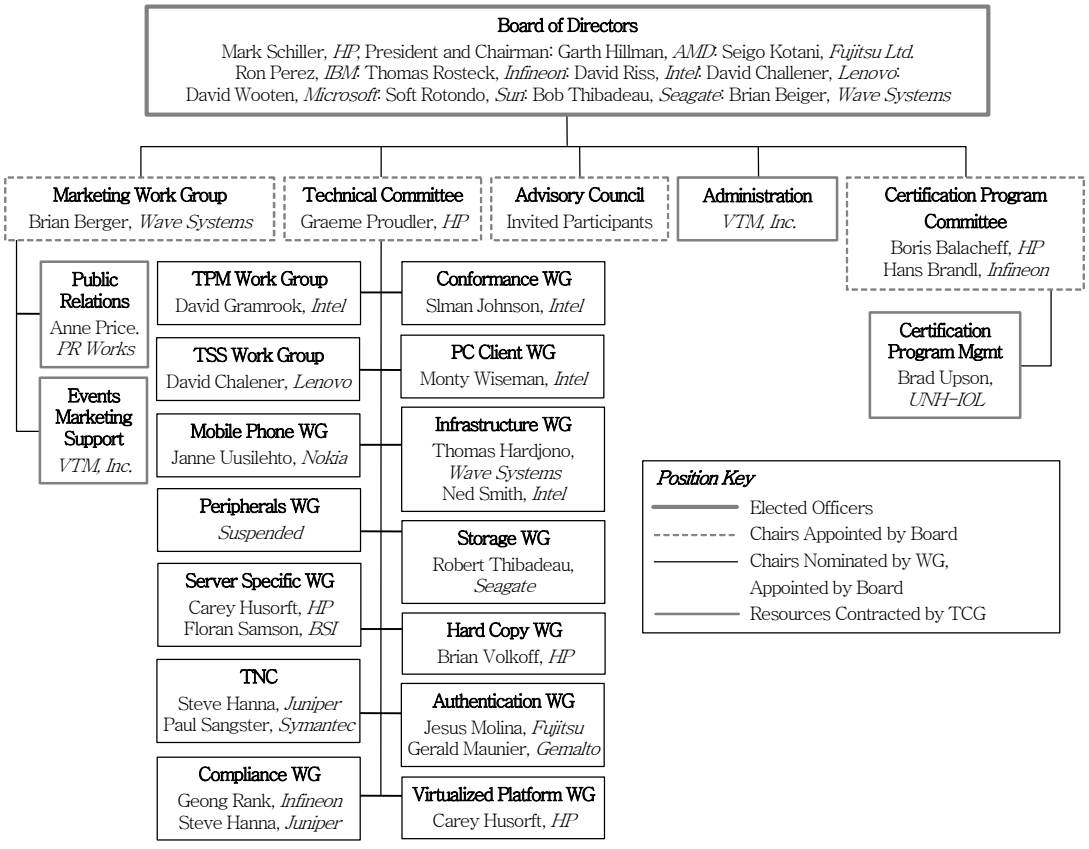
1. 표준화 개요

TCG는 하드웨어 기반의 신뢰 컴퓨팅 및 보안 기술에 대한 산업 표준을 개발, 정의 및 활성화하는 표준화 단체이다. 1999년 Intel, AMD, IBM, HP, Microsoft 등의 대형 업체가 TCPA를 결성하여 신뢰 컴퓨팅에 관한 연구를 진행하였다. 그 후 그 필요성이 부각됨에 따라 2003년 TCG로 확대되었다. 현재 TCG는 전세계 많은 대형 업체들이 표준화에 참여하고 있다.

TCG는 하드웨어에 기반한 신뢰 컴퓨팅 및 보안 기술을 위한 개방형 표준이다. 신뢰 컴퓨팅을 위해 디바이스, 플랫폼, 이들간의 상호 동작, 검증 등의 분야에 대해서 표준화를 진행중이다. TCG의 회원은 TCG의 조직이나 진행되는 표준에 대하여 승인의 권한을 갖는 promoter, 표준화 활동에 직접 참여할 수 있는 contributor, 표준화 활동에 참여하지는 않고 TCG 표준화 내용들을 수용하는 adopter들로 구분할 수 있다. 현재 TCG의 회원사는 총 136개로, 이 중 promoter 8개사, contributor 79개사, adopter 49개사가 회원사로 가입하여 활동하고 있으며, 가입하는 회원이 점점 늘어나는 추세에 있다.

TCG의 조직도는 (그림 7)과 같다. (그림 7)에서 보는 바와 같이 TCG는 BoD 아래에 마케팅 그룹, TC, CPC가 있다.

실제 표준화를 진행하는 곳은 TC 아래에 있는 14개의 WG이다. 회원 자격이 contributor 이상이면 WG에서 표준화 활동을 할 수 있다. 또한 CPC는 2007년에 만들어진 것으로서, TCG 내 모든 워크그



(그림 7) TCG 조직도

룹에 걸친 C&C를 위한 전략, 프로세스 및 구조를 제공하는 역할을 한다. 즉, 각 WG은 C&C 작업을 위해서 CPC와 유기적으로 결합되어 활동하도록 되어 있다.

TCG 내에서는 현재 14개의 WG이 형성되어 활동을 하고 있다. 이들의 역할을 개략적으로 나타내면 <표 1>과 같다.

2. 표준화 현황

현재까지 진행되어 온 TCG 표준화 규격들을 기술하면 <표 2>와 같다. TPM1.2 버전 규격이 제시하는 기능들은 많은 PC 및 노트북 단말에 탑재되어 있는데, 본 절에서는 각 워크그룹별 핵심이 되고 있는 이슈들을 기술하기로 한다.

〈표 1〉 TCG WG의 역할

WG	관심 사항
TPM	TPM의 내부 동작을 정의하는 그룹(특정 기능을 수행하는 데 필요로 하는 입출력과 ordinal을 정의)
TSS	TPM/MTM 칩과 상위 응용이 통신하는 데 필요한 인터페이스 규격을 정의하는 그룹
Mobile Phone	TPM을 모바일 단말에 적용하기 위한 구조 및 명령을 정의하는 그룹
Storage	디스크 드라이브, 제거 가능한 미디어 드라이브, 플래시 스토리지 같은 전용 스토리지 시스템 상의 보안 서비스를 위한 표준화를 진행하는 그룹
PC Client	RoT를 형성하기 위해 TCG 컴포넌트를 사용하는 PC 클라이언트를 위한 공통된 기능, 인터페이스, 보안 및 프라이버시 요구사항을 정의하는 그룹
Server Specific	TCG의 컴포넌트와 방법을 사용하여 신뢰성 있는 서버들을 구축하기 위한 요구사항들을 명시하는 작업을 진행하는 그룹
Virtualized Platform	가상화된 신뢰 플랫폼과 그들의 호스트 플랫폼의 신뢰 특성들에 관한 작업을 진행하는 그룹
TNC	네트워크 액세스 제어(NAC)를 위한 표준들을 생성하는 그룹
Infrastructure	신뢰성 있는 플랫폼의 개발, 관리 생명 주기를 보조하는 규격들을 정의하는 그룹(신뢰성 있는 플랫폼 credential, 백업과 이동을 위한 키 관리, 측정값을 검증할 수 있도록 하는 무결성 관리 기법, TPM의 생명 주기 관리 및 신뢰성 있는 플랫폼 기반 구조 등에 관한 표준화 작업 진행)
Authentication	인증 자체에 관한 표준 규격을 만들고 TPM을 사용한 인증 정책에 대한 표준 규격을 만드는 그룹
Compliance	TCG 관련 제품의 기능적 정확성, 완성도, 상호운용성에 관한 평가와 보증에 관한 작업을 진행하는 그룹
Security Evaluation	PC 및 랩톱에 있는 TPM을 위한 common criteria protection profile의 상세한 규격을 만들어 내는 그룹
Peripherals	주변 장치들의 신뢰 관련 속성들을 식별하고 그들이 동작하는 다양한 환경을 연구하는 그룹
Hardcopy	RoT 생성을 위해 TCG 컴포넌트를 사용하는 하드카피 시스템의 컴포넌트들을 위한 규격을 정의하는 그룹

〈표 2〉 워크그룹별 표준화 현황

WG	표준화 규격
TSS WG	• TCG Software Stack(TSS) Specification Version 1.2 • TCG Software Stack(TSS) Specification Version 1.2 Header Errata 1
PC Client	• TCG Platform Reset Attack Mitigation Specification, Version 1.0 • TCG Physical Presence Interface Specification Version 1.0 • TCG EFI Platform Specification Version 1.2 • TCG EFI Protocol Specification Version 1.2 • TCG PC Specific Implementation Specification Version 1.1 • TCG PC Client Specific TPM Interface Specification(TIS) Version 1.2 • TCG PC Client Specific Implementation Specification for Conventional Bios Version 1.2 • TCG Protection Profile PC Client Specific Trusted Platform Module, TPM Family 1.2, Level 2 Version 0.94

(뒤에 계속)

(계속)

WG	표준화 규격
Server Specific WG	• Mandatory and Optional TPM Commands for Servers Version 1.0, Revision 1.1 • TCG Generic Server Specification Version 1.0 • TCG EFI Protocol Specification, Version 1.2 • TCG EFI Platform Specification Version 1.2 • TCG Itanium Architecture Based Server Specification Version 1.0 • TCG ACPI General Specification Version 1.0
TNC WG	• TCG TNC Architecture for Interoperability Version 1.3 • TCG TNC IF-MAP Binding for SOAP Version 1.0 • TCG TNC IF-IMC Specification Version 1.2 • TCG TNC IF-IMV Specification Version 1.2 • TCG TNC IF-PEP: Protocol Bindings for RADIUS Version 1.1 • TCG TNC IF-T: Protocol Bindings for Tunneled EAP Methods Version 1.1 • TCG TNC IF-TNCCS: Protocol Bindings for SoH Version 1.0
Mobile Phone WG	• TCG Mobile Reference Architecture Version 1.0 • TCG Mobile Trusted Module Specification Version 1.0
Infra-structure WG	• TCG Credential Profiles Specification Version 1.1, Revision 1.014 • Security Qualities Schema Specification Version 1.1, Revision 7 • Verification Result Schema Specification Version 1.0, Revision 1.0 • Core Integrity Schema Specification, Version 1.0.1, Rev 1.0 • Integrity Report Schema Specification Version 1.0, Rev. 1.0 • Reference Manifest(RM) Schema Specification Version 1.0, Rev. 1.0 • Simple Object Schema Specification Version 1.0, Rev. 1.0 • Architecture Part II - Integrity Management Version 1.0, Rev. 1.0 • Infrastructure Subject Key Attestation Evidence Extension Version 1.0 • Interoperability Specification for Backup and Migration Services Version 1.0 • Platform Trust Services Interface Specification(IF-PTS), Version 1.0, Rev 1.0 • Reference Architecture for Interoperability Version 1.0
TPM WG	• TCG TPM Specification Version 1.2 Revision 103: Design Principles, Structures of the TPM, Commands

가. TPM WG

TPM WG은 TPM의 내부 기능을 정의하는 그룹이다. 현재 1.2 버전은 거의 완성되었으며, 그 다음 버전인 TPM.Next에 대한 논의가 2007년부터 활발히 진행되어 오고 있다. TPM.Next의 핵심 이슈들은 1.2 버전에서 지원하는 암호 알고리듬의 약점을 개선하기 위한 암호 알고리듬의 확장 지원, 1.2 버전의 BLOB 구조 개선, GA를 위한 명령어 규격화 등으로 요약할 수 있다.

그러나, TPM.Next 작업은 방대하고 많은 논의를 필요로 해서 규격화가 완성될 때까지는 많은 시간이 필요하므로 TPM 1.2의 약점들을 개선한 버전의 규격을 만들어서 공표하자는 의견들이 수렴되었다. 이를 TPM 1.3으로 명명하여 진행중이다.

나. TSS WG

TPM 1.2에 해당하는 TSS 규격은 완성되었고, TPM.Next에 대응하는 TSS.Next 규격은 0.24 버전까지 완성된 상태이다. TSS.Next는 TPM.Next의 기능과 MPWG의 MTM 규격에서 정의한 기능들을 반영하여 구성되어 있다. 현재 TSS WG의 활동은 거의 없는 상태이다. TPM WG에서 TPM 1.3 버전 규격의 작업과 더불어 TSS WG의 TSS 1.3 작업도 진행될 것으로 판단된다[8].

다. PC Client WG

RoT를 형성하기 위해 TCG 컴포넌트를 사용하는 PC 클라이언트를 위한 공통된 기능, 인터페이스, 보안 및 프라이버시 요구사항을 정의하는 그룹이다.

세부 항목을 살펴보면, TIS, 리셋 공격, migration, physical presence 인터페이스, EFI 프로토콜, EFI 플랫폼, conventional BIOS 등에 대한 규격화 작업을 진행하였다. 현재는 PC-TPM간의 compliance 시험을 위한 테스트 계획에 대해 논의중이다.

라. Server Specific WG

TCG의 컴포넌트와 방법을 사용하여 신뢰성 있는 서버들을 구축하기 위한 요구사항들을 명시하는 작업을 진행하는 그룹이다. 서버 구조, EFI 프로토콜 및 플랫폼 규격을 포함하여 기본적인 규격은 이미 공표되어 있으며, 현재는 사용자 시나리오, 서버와 TPM간의 C&C 전략에 관해 논의되고 있는 중이다.

마. TNC WG

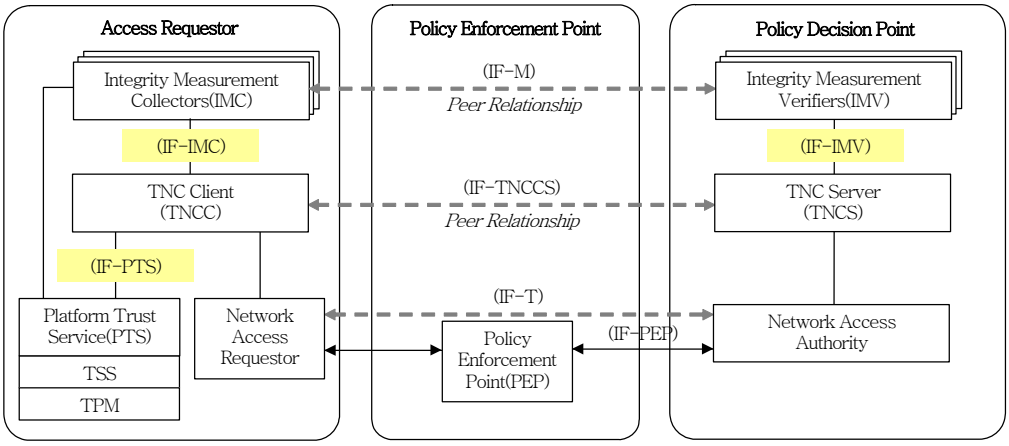
네트워크 액세스 제어(NAC)를 위한 표준들을 생성하는 그룹이다. 이 규격들은 네트워크로의 액세스를 부여할 때 종점의 무결성에 관한 정책을 네트워크 운영자들이 시행할 수 있도록 한다. 현재 75개 이상의 회원사가 TNC를 지원하고 있다. IF-IMV, IF-IMC, IF-M, IF-MAP, IF-PEP, IF-PTS, IF-SIG, IF-T, IF-TNCCS, IF-TNCS 등 다양한 규격이 정의되어 있다. (그림 8)의 TNC 구조를 참조하면 규격의 역할을 보다 쉽게 이해할 수 있다.

바. Mobile Phone WG

MPWG는 TPM을 모바일 단말에 적용하기 위한 구조 및 명령을 정의하는 그룹이다. 이 그룹은 <표 2>에 기술되어 있듯이 MTM 규격과 RA 규격 1.0을 공표하였다. 현재 이들에 대한 논의는 계속되고 있지만, 전체적인 구조와 기능은 완성된 상태이다. 현재, TSS의 TDDL과 TCS에 해당하는 인터페이스와 기능 구조를 정의하는 MTM abstraction layer에 대한 규격화 작업이 2008년 하반기에 진행될 예정이다[9]-[11].

MPWG에서는 이 외에도 사용 예(use case) 분석, compliance, 안전성 평가(security evaluation) 작업이 진행되고 있다. 사용자 시나리오 분석 문서는 사용자 시나리오 문서에서 기술된 모든 경우들을 분석할 때까지 기다리기보다 현재까지 분석된 내용을 정리해서 1.0 버전을 빨리 공표하자는 게 회원들의 공통된 생각이며, 조만간 완성될 것으로 전망된다.

Conformance 관련 작업은 핵심 문서(core document), MLTM과 MRTM을 위한 추가 문서(addendum)들에 대한 0.01 버전이 만들어진 상태이다. Compliance 작업과 관련된 요구사항 문서는 0.03 버전이 현재 논의중이며 test suite 개발 작업은 2009년 1/4분기까지 완성될 것으로 전망된다.



(그림 8) TNC WG의 구조

사. Infrastructure 표준화 동향

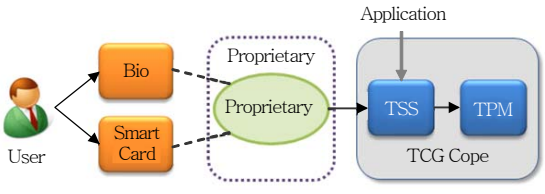
IWG는 신뢰성 있는 플랫폼의 개발, 관리 생명 주기를 보조하는 규격들을 정의하는 그룹이다. 이 그룹에서는 신뢰성 있는 플랫폼 credential, 백업과 이동을 위한 키 관리, 측정을 검증할 수 있도록 하는 무결성 관리 기법, TPM의 생명주기 관리 및 신뢰성 있는 플랫폼 기반 구조 등에 관한 표준화 작업이 진행되어 왔고 많은 규격들이 완성되어 공표되어 있는 상태이다.

3. 향후 쟁점 사항

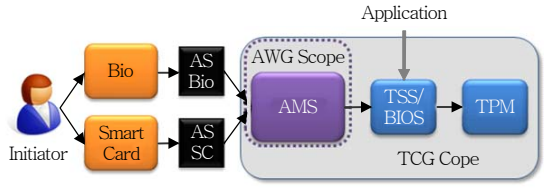
가. Authentication WG

AWG는 2007년 1월에 조직된 그룹으로, Broadcom, Fujitsu, Gemalto, NTRU, Wave Systems, AuthenTec 등의 업체들이 활동중이다. AWG는 (그림 9)에서와 같이 비 패스워드 기반의 인증 소스들이 TSS나 TPM과 상호 동작하는 데 필요한 API를 정의하는 그룹이다.

RA, 인터페이스, GA에 관한 표준화 작업이 진행중이고, 아직 공표된 규격은 없다.



(a) Current Status



(b) AWG Architecture

(그림 9) AWG의 관심 영역

나. Virtualized Platform WG

VPWG은 2007년 10월에 공식적으로 형성되어 활동중이다. 이 그룹에서는 가상화된 신뢰 플랫폼과 그들의 호스트 플랫폼의 신뢰 특성들에 관한 작업을 하는 것이 이 그룹의 역할이다. 현재 가상화된 플랫폼 규격화 작업이 진행중이다.

다. Compliance WG

TCG 관련 제품의 기능적 정확성, 완성도, 상호운용성에 관한 평가와 보증에 관한 작업을 진행하는 그룹이다. 따라서 TCG 내의 모든 WG와 관련이 있다. 이 그룹에서는 compliance 테스트를 위한 공통적인 요구사항, test plan 문서 등을 규격화하고 테스트를 진행해야 하는 개별 WG에 대해서는 서브 그룹을 생성하여 진행하도록 한다. 현재 Compliance_PC-TPM, Compliance_TNC 서브그룹이 형성되어 활동하고 있다. 이는 두 WG의 규격들이 거의 진행이 되었음을 의미한다.

라. Security Evaluation WG

현재 TCG에서 가장 관심을 갖는 이슈가 공통기준(Common Criteria)이다. SEWG에서는 TPM 관련 제품들의 보안 기능이 완벽히 제공되고 있는지 시험하는 것에 관심이 있으며, 이와 가장 관련이 있는 것이 공통기준이다. 이에 대해서는 아직 많은 논의가 남아 있는 상태이다.

Ⅳ. 결론

TC 기술은 IT security 전반에 활용될 수 있는 핵심 기술로 컴퓨터, 통신분야의 주요 연구기관 및 관련업체들이 동참하여 개방형 표준으로 만들어가고 있는 기술이며, TCG는 다른 표준 단체에서 다루

● 용 어 해 설 ●

IMA(Integrity Measurement Agent): 플랫폼에서 수행되는 혹은 수행될 소프트웨어가 신뢰할 수 있는지 검사하기 위해 플랫폼상에 상주하며 소프트웨어의 무결성을 검증하고 기록하는 역할을 담당하는 에이전트

지 못했던 신뢰성 확립을 위한 다양한 요소 기술을 제시하고 그와 관련된 내용을 표준화하는 역할을 담당한다.

본 기고에서는 TC 기술이 가지는 독창적인 특징에 대해 구체적으로 설명하였고, 관련 표준화 활동의 전반에 대하여 개괄적으로 정리하여 소개하였다.

향후 쟁점 사항이 되고 있는 부분에 대하여는 지속적인 연구 및 개발이 필요하며 TC 기술이 지닌 단점을 극복할 수 있는 새로운 대안이 요구된다.

또한, 표준화에 적극적으로 동참하여 신뢰할 수 있는 인터넷 세상을 만들어 갈 수 있도록 많은 노력을 기울여야 할 것이다.

약 어 정 리

AIK	Attestation Identity Key
AMS	Authentication Management System
AS	Authentication Source
BBB	BIOS Boot Block
BoD	Board of Director
C&C	Conformance & Compliance
CA	Certification Authority
CPC	Certification Program Committee
CRTM	Core Root of Trust for Management
DAA	Directed Anonymous Attestation
DES	Data Encryption Standard
EFI	Extensible Firmware Interface
EK	Endorsement Key
GA	Generalized Authorization
HMAC	Hash-based Message Authentication Code
IMVA	Integrity Measurement Verification & Agent
MLTM	Mobile Local-Owner Trusted Module
MRTM	Mobile Remote-Owner Trusted Module
MTM	Mobile Trusted Module
NAC	Network Access Control
NV	Non-Volatile
PCR	Platform Configuration Register
Privacy-CA	Privacy Certificate Authority
RA	Reference Architecture
RNG	Random Number Generator
RoT	Root of Trust
RSA	Rivest, Shamir and Adleman
RTM	Root of Trust for Management
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
SHA-1	Secure Hash Algorithm-1
SoC	System on Chip
SRK	Storage Root Key
TC	Trusted Computing
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TCS	TSS Core Services
TDDL	TPM Device Driver Library
TIS	TPM Interface Specification
TPM	Trusted Platform Module
TSP	TSS Service Provider
TSS	TCG Software Stack
WG	Work Group

참 고 문 헌

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

[2] C. Mitchell ed., *Trusted Computing*, London, UK: IEE Press, 2005.

[3] 김영수, 박영수, 박지만, 김무섭, 김영세, 주홍일, 김명은, 김학두, 최수길, 전성익, "신뢰 컴퓨팅과 TCG 동향," 전자통신동향분석, 제22권 제1호, 2007. 2., pp.83-96.

[4] Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn: *Design and Implementation of a TCG-based Integrity Measurement Architecture*, *13th Usenix Security Symp.*, Aug. 2004.

[5] Trusted Computing Group: *TCG Specification Architecture Overview*. Specification Revision 1.4, Aug. 2, 2007, www.trustedcomputinggroup.org

[6] 김무섭, 신진아, 박영수, 전성익, "모바일 플랫폼용 공통보안핵심 모듈 기술," 정보보호학회지, 제17권 제3호, 2006, pp.7-17.

[7] FIPS, "*Specification for the Secure Hash Standard*," Tech. Rep. 180-2, National Technical Information Service(NTIS), Aug. 2002.

[8] Trusted Computing Group: *TCG Software Stack*, Specification version 1.2, Mar. 7, 2007.

[9] Trusted Computing Group: *TCG Mobile Reference Architecture*. Specification version 1.0, Revision 1, June 12, 2007.

[10] Trusted Computing Group: *TCG Mobile Trusted Module Specification,* Specification version 1.0, Revision 1, June 12, 2007.
[11] E. Gallery and C.J. Mitchell, "Trusted Mobile Platforms," *in FOSAD '07, Int'l School on Foundations of Security Analysis and Design*, Vol.4677 of LNCS, Springer-Verlag, Sep. 2007.