신뢰 컴퓨팅기술 기반 SaaS 인증 및 과금 플랫폼 구조 설계

이상환*, 김정윤**, 전성익***
*국민대학교 컴퓨터학부, **민족사관고등학교, ***한국전자통신연구원
e-mail:sanghwan@kookmin.ac.kr

SaaS Platform Structure Design for Authentication and Accounting based on Trusted Computing Technology

Sang Hwan Lee*, Jane Chungyoon Kim**, Sungik Jun***
*Dept. of Computer Science, Kookmin University
**Korean Minjok Leadership Academy
***Electronics and Telecommunications Research Institute

요 약

최근 컴퓨터 기술의 발전과 네트워크의 개방화 그리고 무선 모바일 통신 기술의 비약적인 보급으로 인하여 컴퓨팅 환경을 이루고 있는 각종 장치(PC, 모바일 단말, 저장장치, 네트워크 기기 등)가 다양한 형태의 보안 위협에 노출되어 데이터의 유실, 조작, 유출되어 금전적인 피해를 입거나 프라이버시 침해를 받고 있다. 이러한 문제를 근본적으로 해소하기 위하여 설립된 TCG(Trusted Computing Group)는 세계적인 IT 핵심기업들을 중심으로 구성된 비영리 단체로서 PC 혹은 모바일 기기 등의 단말과 서버 장비 그리고 저장 장치 및 네트워크로 구성된 컴퓨팅 환경에서 보안성 향상 및 데이터의 신뢰성을 제고하기 위하여 TPM(Trusted Platform Module)이라는 반도체 칩을 신뢰의 기반(root of trust)으로 한 신뢰 플랫폼을 제안하고 있다.

한편 SaaS(Software as a Service)는 패키지 형태의 소프트웨어를 네트워크 서비스 형태로 바꾸어 사용량에 비례한 요금제로 과금하는 방식을 채택하고 사용자가 온디맨드로 요청한 서비스를 적시에 제공하는 기술로 최근 전세계적으로 각광을 받고 있다. 이때 다양한 컴퓨팅 환경 안의 사용자에게 높은 신뢰성과 보안성 그리고 연속성을 갖는 SaaS 서비스를 제공하고 데이터의 무결성 및 비밀유지와 정확한 서비스 사용시간을 기록하고 업로드하는 기능들을 제공하는 SaaS 플랫폼은 TPM기반의 신뢰 컴퓨팅 기술을 통하여 쉽게 구현될 수 있다.

본 논문에서는 일시적으로 네트워크와 차단된 상태의 PC 혹은 모바일 단말에서도 위의 조건들을 만족하는 SaaS 서비스를 지원하는 신뢰 플랫폼이 가져야 할 기능들에 대하여 분석-도출한 후 그러한 기능들을 제공하는 컴포넌트로 구성된 신뢰형 SaaS 사용자 플랫폼을 설계하였다.

1. 서 론

최근 컴퓨터 기술의 발전과 네트워크의 개방화 그리고 무선 모바일 통신 기술의 비약적인 보급으로 인하여 컴퓨팅 환경을 이루고 있는 각종 장치(PC, 모바일 단말, 저장장치, 네트워크 기기 등)가 다양한 형태의 보안 위협에 노출되어 데이터의 유실, 조작, 유출되어 금전적인 피해를 입거나 프라이버시 침해를 받고 있다. 이와 같이 심각한 상태에 놓인 보안 문제를 근본적으로 해소하기 위하여 설립된 TCG(Trusted Computing Group)[1,2]는 신뢰성 있는 컴퓨팅 환경의 제공을 목표로 세계적인 IT 핵심 기업들을 중심으로 구성된 비영리 단체로서 PC 혹은 모바일 기기 등의 단말과 서버 장비 그리고 저장 장치 및 네트워크로 구성된 컴퓨팅 환경에서 보안성 향상 및 데이터의 신뢰성을 제고하기 위하여 TPM(Trusted Platform Module)이라는 반도체 칩을 신뢰의 기반(root of trust)으로 한 신뢰 플랫폼을 제안하고 있는데, 현재 TPM을 탑재한 PC 및 모바일 PC가 전세계적으로 연간 수천만대에 이르고 있으며 국내 시장에서도 보급되고 있다.

한편 SaaS(Software as a Service)[6]는 패키지 형태의 소프트웨어를 네트워크 서비스 형태로 바꾸어 사용량에 비례한 요금제로 과금하는 방식을 채택하고 사용자가 온디맨드로 요청한 서비스를 적시에 제공하는 기술로 최근 전세계적으로 각광을 받고 있다[7,8]. SaaS 기술의 장점은 서비스 개발자에게는 공통 플랫폼 및 API 인프라를 제공함으로 소프트웨어 재사용성을 높이고, 서비스 유지 보수 및 업그레이드에 있어서 네트워크를 통한 원스톱(One-Stop) 처리가 가능하게 되어 소프트웨어 유지보수 비용을 대폭 절감시켜주며, 서비스 제공자에게는 수많은 서비스들을 간단한 절차로 통합 제공하는 기반을 제공할 뿐만 아니라 사용자에게는 통일된 환경하에서 서비스 간 정보교환을 원활하게 해주어 업무능률을 향상시키도록 해준다. 이때 다양한 컴퓨팅 환경 안의 사용자에게 높은 신뢰성과 보안성 그리고 연속성을 갖는 SaaS 서비스를 제공하고 데이터의 무결성 및 비밀유지와 정확한 서비스 사용시간을 기록하고 업로드하는 기능들을 제공하는 SaaS 사용자 플랫폼은 TPM기반의 신뢰 컴퓨팅 기술을 통하여 쉽게 구현될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 TPM 기반의 신뢰플랫폼에 대하여 소개한다. 3장에서는 본 논문에서 사용하는 SaaS 모델을 설명한다. 4장에서는 네트워크 비접속 상태에서도 SaaS 서비스를 신뢰성 있게 연속적으로 제공하는 컴퓨팅 환경을 구현하는데 필요한 기능을 도출하고, 그러한 기능을 제공하는 컴포넌트로 구성된 신뢰형 SaaS 사용자 플랫폼을 제안한다. 마지막으로 5장에서는 본 논문의 결론 및 향후 과제에 대하여 논한다.

2. TPM 기반 신뢰 플랫폼 소개

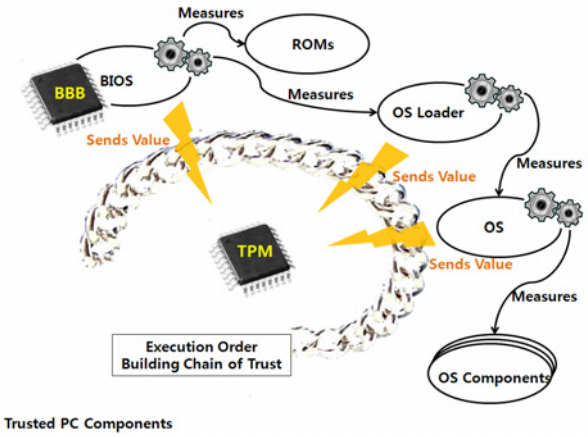
이번 절에서는 본 논문에서 사용하는 신뢰성 제공기술인 TPM 기반 신뢰 플랫폼[3]에 대해 설명한다. 본 기술은 2003년 TCG(Trusted Computing Group)에 의하여 제안되고 있는 신뢰 컴퓨팅 기술로서 현재 전세계적으로 160여 기관들로 구성되어 있다.

2.1 TPM

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 설계기술을 요구한다. TPM은 또한 칩 자체에 대한 물리적인 공격에 대처하기 위한 센서와 내부 보안 구조(예를 들면, 칩의 최상위 와이어 계층의 액티브 스크린)로 되어 있어 내부에 저장된 보안 정보들의 누출이 현실적으로 불가능하도록 제작되어 있다.

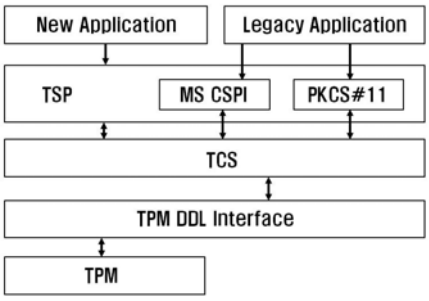
2.2 TPM 기반 안전 부팅 기능

플랫폼 무결성 측정[4,5]은 신뢰 플랫폼이 제공하는 가장 중요한 기능 중 하나이다. PC에 전원이 들어오는 순간 ROM 등의 수정 불가능 영역에 저장되어 있는 안전 부팅코드가 최초로 실행되면 부팅코드는 (그림1)에서와 같이 다음단계의 실행코드인 OS Loader의 코드값을 처리하여 측정치를 생성한 후에 TPM 내에 저장되어 있는 기대치와 비교한다. 이때 두개의 값이 다르면 OS Loader는 바이러스 등에 의하여 변경되었다고 판단하여 시스템 부팅과정을 취소하여 오염된 컴퓨팅 환경의 발생을 차단한다. 위의 두 값이 같으면 OS Loader는 정상적인 로딩 기능을 수행한 후 운영체계(OS)코드에 대한 측정치를 계산한 후 기대치와 비교하는 과정을 통하여 올바른 운영체계만이 실행되는 환경을 구축한다. 운영체계가 응용 소프트웨어를 실행할 때에도 이러한 무결성 측정을 통하여 모든 실행 소프트웨어에 대한 신뢰체인을 형성함으로써 전체 플랫폼의 안전성을 확보·유지한다.



(그림1) TPM 기반 안전 부팅 과정

2.3 TPM 기반 신뢰 플랫폼



(그림2) TPM기반 신뢰 플랫폼

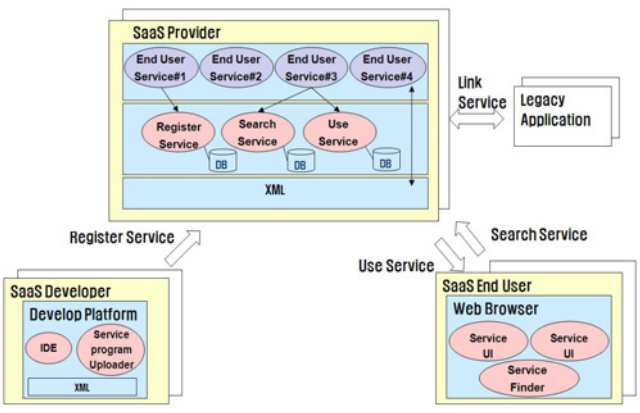
TPM 기반 신뢰 플랫폼은 (그림2)와 같이 특정 드라이버와 관련 운영 체제에 TPM 함수들을 제공하는 보안API 등으로 구성된다. 플랫폼의 목적은 애플리케이션에게 TPM 기능에 대한 단일 엔트리 포인트를 제공하고, TPM에 대한 동기화된 액세스를 제공하며, 명령어 스트림을 정확한 바이트 오더링으로 숨기고, TPM 리소스를 관리하는 것이다.

최하위 레벨에서 플랫폼은 인터페이스를 초기화하고 LPC 버스를 통해 TPM과 데이터를 교환하는 하드웨어 기반 디바이스 드라이버(커널 모드)로 구성된다. 그 다음 상위 레벨은 TPM Device Driver Library (TDDL)로서 TDDL은 TPM 애플리케이션에 대하여 운영체제 독립적인 인터페이스를 제공하며, 여러 TSS 구현들이 어떠한 TPM과도 정확히 통신할 수 있도록한다. TSS Core Services (TCS)는 일반 플랫폼 서비스들에 대한 인터페이스를 제공한다. 하나의 플랫폼에 여러 개의 TSP가 있다고 하더라도, TCS는 모든 TSP들이 정상적으로 동작하도록 한다. TSS Service Provider (TSP)는 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 제공한다. 암호 서비스는 TPM 보호 기능을 효율적으로 사용하기 위해 암호 기능을 제공하며 기존 두 개의 표준 API(MS CSPI, PKCS#11)가 적용될 수 있다.

3. SaaS 모델

이번 절에서는 본 논문에서 사용하는 SaaS모델을 소개한다.

3.1 SaaS 전체 시스템 구조

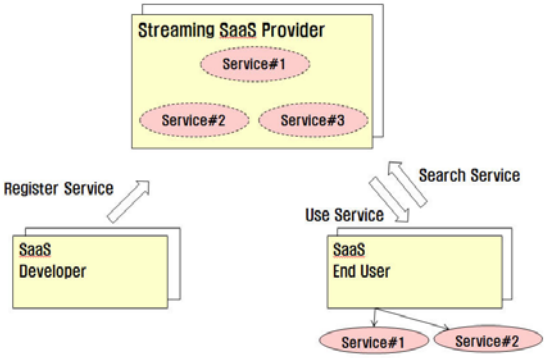


(그림3) SaaS 전체 시스템 구조

(그림3)은 SaaS 전체 시스템 구조도를 보여준다. 모든 소프트웨어는 서비스의 형태로 사용자에게 제공된다. SaaS Developer는 서비스 소프트웨어를 Developer Platform에서 개발한 후 SaaS Provider Platform에 옮긴 다음 사용자의 접속을 기다린다. 사용자는 서비스 검색도구와 서비스 연동도구 등을 통하여 원하는 서비스들을 발견한 후 연동하여 사용한다.

3.2 SaaS 모바일 서비스 제공 구조

(그림4)는 SaaS 모바일 서비스 제공 구조를 나타낸다. 사용자는 필요에 따라서 모바일 디바이스를 통하여 장소를 이동하면서 서비스를 사용할 필요가 있다. 이때 네트워크 접속이 일시적으로 차단되어도 서비스를 계속적으로 사용하게 해주는 모바일 플랫폼이 필요하다. 이러한 서비스를 지원하는 기술로 소프트웨어 스트리밍의 에버그린 기술과 클라이언트와 서버 환경을 하나의 디바이스 내에서 통합 지원하는 기술 등이 존재한다.



(그림4) SaaS 모바일 서비스 제공 구조

4. TPM 기반 신뢰형 SaaS 플랫폼 설계

이번 절에서는 본 논문에서 제안하는 TPM 기반 신뢰형 SaaS 플랫폼을 설계한다.

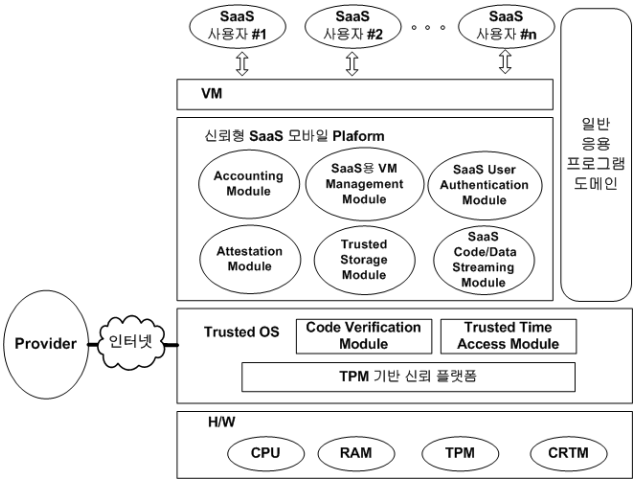
4.1 신뢰형 SaaS 플랫폼 요구 기능

SaaS 서비스가 네트워크에 연결된 상태의 PC뿐만 아니라 네트워크와의 연결이 일시적으로 차단된 형태에서도 서비스가 연속적으로 진행되기 위해서는 서비스 제공 소프트웨어가 사용자 단말(PC, 노크북, 모바일 단말 등)에도 설치되어 있어야 한다. 이때 사용자 단말에 설치된 서비스 소프트웨어는 사용자와 제공자 간에 약속된 규정에 따라서 사용시간에 비례한 서비스요금이 사용자도 안심하고 인정할 수 있도록 과금하여야 한다. 또한 서비스 소프트웨어가 불법으로 복사되거나 사용자의 정보가 무단으로 노출 및 유출되는 것을 방지하는 장치가 필요하다. 다음은 고정/모바일 서비스를 동시에 제공하는 신뢰형 SaaS 플랫폼 요구기능들을 나열하고 있다.

- 네트워크 연결에 무관한 서비스 연속실행 기능
- 데이터 암호화 기능
- 데이터 불법 복제/유출 방지 기능
- 데이터 안전 업로드/다운로드 보안 기능
- 사용자 단말 H/W 및 S/W 플랫폼 검증 기능
- 서비스 S/W 안전 다운로드 및 복제방지 기능
- 사용자-제공자 상호 신뢰형 공정 과금 기능

4.2 신뢰형 SaaS 플랫폼 구조

사용자 단말이 TPM 칩을 장착한 상태에서 TPM 기반 신뢰 플랫폼을 정상적으로 구축·유지하는 경우, 네트워크와 연결된 상태의 사용자 단말은 기본적으로 위의 요구기능들을 쉽게 구현하는 신뢰 환경을 제공할 수 있다. 그 구체적인 방법에 대해서는 참고문헌에 소개되어 있다. 따라서 본 절에서는 네트워크와의 연결이 중단된 상태에서도 위의 기능들을 정상적으로 제공하는데 필요한 컴포넌트들에 대하여 좀더 자세히 설명한다. (그림5)는 본 논문에서 제안하는 신뢰형 SaaS 모바일 플랫폼 구조를 보여준다.



(그림5) 신뢰형 SaaS 모바일 플랫폼 구조

그림에서 사용자가 모바일 단말에서 일시적인 네트워크 차단상태에서도 임의의 서비스를 사용하고자 하는 경우 사용자는 SaaS Code/Data Streaming Module을 통하여 미리 서비스 프로그램 코드를 다운로드 받는다. 이때 SaaS 서비스 Provider는 사용자 단말이 TPM기반 신뢰플랫폼을 정상적으로 구현하고 있는지 확인하기 위하여 Attestation Module을 통하여 TPM플랫폼 상태를 원격 검증한 후 정상적인 경우에 한하여 해당 서비스 코드 및 데이터를 다운로드한다. 다운로드 후 모바일 플랫폼은 필요시 VM Management Module을 통하여 가상 운영체계를 실행한 후 그 안에서 서비스 프로그램을 실행함으로서 SaaS 서비스 실행을 단말내 기존 컴퓨팅 환경과 차단하여 상호 안전을 도모한다. 한편 모바일 단말은 자체 신뢰도를 유지하기 위하여 운영체계내의 Code Verification Module을 통하여 다운로드된 코드의 신뢰도를 인증기관으로부터 확인할 수 있다. 필요시 모든 데이터는 Trusted Storage Module을 통하여 TPM 암호화된 상태로 사용 및 저장되도록 하여 모바일 단말이 사용자 소유가 아닌 상황에서도 비밀을 유지할 수 있도록 한다. SaaS Accounting Module은 사용자의 서비스 이용 시간 정보를 주기적으로 기록하고 Provider에게 Reporting하여 올바른 과금을 수행하는데 이때 정확한 시간 정보를 얻기 위하여 TPM자체의 Timer기능이나 이미 신뢰평가를 거친 상태의 운영체계의 Trusted Time Access Module을 사용한다.

마지막으로 신뢰 플랫폼 개념은 Provider 측에도 적용되어 사용자가 안심하고 자신의 데이터를 Provider에서 처리 및 저장을 하도록 할 수도 있다.

5. 결 론

본 논문에서는 우선 TPM 기반의 신뢰플랫폼에 대하여 소개하였고 이어서 본 논문에서 사용하는 SaaS 모델을 설명한 다음 네트워크 비접속 상태에서도 SaaS 서비스를 신뢰성 있게 연속적으로 제공하는 신뢰 컴퓨팅 환경을 구현하는데 필요한 기능을 도출하였고 마지막으로 그러한 기능을 제공하는 컴포넌트로 구성된 신뢰형 SaaS 플랫폼을 제안하였다. 향후 연구로 ETRI에서 제작한 TPM칩 및 보안 프레임워크 상에서 본 논문에서 제안하는 신뢰형 SaaS 플랫폼을 구현하는데 필요한 요구사항을 도출할 예정이다.

감사의 글

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음.
[2006-S-041-02, 차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통 보안 핵심 모듈 개발]

참고문헌

[1] S.W. Smith, “Trusted Computing Platforms: Design and Applications,” Springer, 2005.
[2] Trusted Computing Group Website, http://www.trustedcomputinggroup.org
[3] 김영수, 박영수, 박지만, 김무섭, 김영세, 주홍일, 김명은, 김학두, 최수길, 전성익, “신뢰 컴퓨팅과 TCG 동향,” 전자통신동향분석 제22권 제1호, 2007. 2.
[4] 김무섭, 신진아, 박영수, 전성익, “모바일 플랫폼용 공통보안핵심 모듈 기술,” 정보보호학회지 제16권 제3호, 2006.6.
[5] HongIl Ju, SungIk Jun, “A Study on Secure Boot for Mobile Platform”, 2006
[6] Mark Turner, David Budgen, Pearl Brereton, “Turning Software into a Service”, Keele University, Staffordshire, IEEE Computer Society, 2003
[7] 문병주, “SaaS(Software as a Service) 동향“, IITA 주간기술동향 통권 1306호, 2007.7.25
[8] Mackinsey & SandHill Group, “Software 2006 Industry Report”, 2006