TPM 을 이용한 신뢰컴퓨팅기반 SaaS 모델 설계 및 구현

김영만*, 전성익**, 김은석*, 정혜영*
*국민대학교 컴퓨터공학부
**한국전자통신연구원)
e-mail : ymkim@kookmin.ac.kr*

Design and Implementation of SaaS Model based on Trusted Computing Technology using TPM

Young Man Kim*, Sung Ik Jun**, Eun Seok Kim*, Hye Young Jung*
*Dept. of Computer Science, Kook-min University
** Electronics and Telecommunications Research Institute

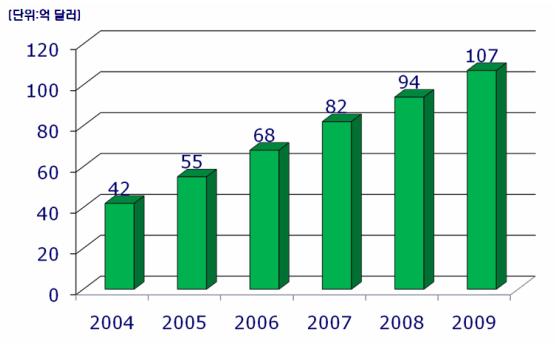
요 약

Web 2.0 시대가 도래하면서부터 새로운 소프트웨어 배포 방식인 SaaS 가 등장하였다. 보안 분야에서도 기존의 소프트웨어적인 보안 방식이 아닌 하드웨어적인 보안 방식을 위해 TPM 이라는 보안 칩이 개발되었다.

본 논문에서는 TPM 칩을 사용하여 보다 신뢰적인 측면이 강조된 신뢰 컴퓨팅 기반 SaaS 모델을 설계하고, 설계된 모델의 가장 기본적인 기능인 로컬 PC 레벨의 PCR 값 인증 프로그램과 로컬 PC 레벨 어플리케이션 무결성 측정 프로그램을 구현하고 이를 평가한다.

1. 서론

최근 소프트웨어 비즈니스 모델은 기존의 소프트웨어 제공방식(패키지 판매-설치-유지보수)에서 벗어나 웹과 인터넷을 이용한 서비스 형태로 소프트웨어를 제공하며, 소프트웨어 사용량에 비례하여 요금을 과금하는 방식인 SaaS(Software as a Service)[1] 모델이 전 세계적으로 각광을 받고 있다[2][3]. 그림 1 은 SaaS 모델의 시장 추이 전망을 나타낸다.



(그림 1) SaaS 모델의 시장 추이 전망

SaaS 모델은 서비스 개발자에게 공통 플랫폼 및 API 인프라를 제공함으로써 높은 소프트웨어 재사용성과 서비스 유지 보수 및 업그레이드에 있어서 편의성을 제공하고, 서비스 제공자에게는 수많은 서비스들을 간단한 절차로 통합하는 기반을 제공한다[4]. 또한 서비스 사용자에게는 인터넷에 접속하여 언제, 어디서나 사용자가 원하는 때에 필요한 만큼 서비스를 사용하고 사용량에 비례하여 비용을 지불하면 된다는 점에서 편의성을 제공한다.

SaaS 모델은 위와 같은 장점과 더불어, 최근 발전된 컴퓨팅 기술과 무선 모바일 통신 기술을 포함한 네트워킹 방식의 보편화, 그리고 각종 단말 장치(PC, UMPC, PDA 등)와 주변장치(저장 장치, 네트워크 기기 등)의 다양화로 인해 높은 비즈니스적 부가가치를 창출할 것으로 예상되고 있다. 이렇듯 고부가가치를 지니고 있는 SaaS 모델은 기존의 소프트웨어적인 보안 방식의 플랫폼을 사용하는 것 보다 한 차원 높은 보안성을 제공할 수 있도록 TCG 에서 제안한 하드웨어적인 보안 방식인 TPM 기반 플랫폼을 사용함으로써 사용자에게 높은 보안과 신뢰성 기반의 서비스를 제공하고 송·수신 데이터의 무결성 및 사용자 정보 보호, 그리고 정확한 서비스 사용 시간 측정 및 기록 등을 보장할 수 있다.

TCG(Trusted Computing Group)[5][6]은 Intel, AMD, IBM, HP 및 MS 등, 세계적인 IT 핵심 기업들을 중심으로 구성된 비영리 단체로써, 각종 데이터를 보호하고, 신뢰성 있는 네트워킹을 위해 하드웨어 기반의 신뢰 컴퓨팅 환경 개발을 목표로 한다. 특히 사용자의 단말 및 주변 장치가 다양한 형태의 보안 위협에 노출되어 발생할 수 있는 데이터의 유실, 조작 유출로 인한 금전적인 피해나 프라이버시 침해를 막기 위해 TPM(Trusted Platform Module)이라는 반도체 칩을 사용한 하드웨어 기반의 신뢰 컴퓨팅을 제안하고 있으며, 현재 TPM 을 탑재한 PC 및 모바일 PC 가 전 세계적으로 연간 수 천만대에 이르고 있다.

본 논문에서는 TPM 을 이용한 신뢰 컴퓨팅 기반

SaaS 모델을 설계하며, 설계된 SaaS 모델을 위한 로컬 PC 레벨 무결성 검증 어플리케이션을 구현하고 이를 평가한다.

2. 관련연구

본 장에서는 신뢰 컴퓨팅 기반 SaaS 모델을 구현하는데 있어서 관련된 연구들을 살펴보도록 한다.

2.1 SaaS

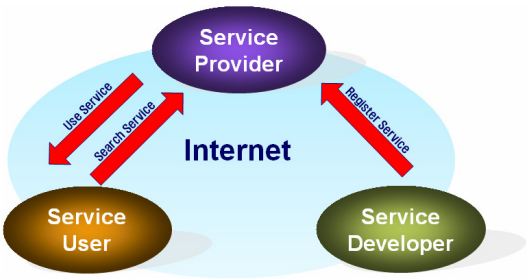
가. SaaS 개요

SaaS 는 하나 이상의 소프트웨어 제공 업체가 원격지에서 보유·제공·관리하는 소프트웨어를 뜻하며, 소프트웨어 제공 업체는 단일 플랫폼을 이용해 다수의 고객에게 소프트웨어 서비스를 제공하며, 사용자는 소프트웨어를 이용한 만큼 돈을 지불(pay-as-you-go)하면 되는 서비스를 뜻한다. 전통적인 소프트웨어 비즈니스 모델과 비교했을 때, SaaS 는 소프트웨어를 패키지가 아닌 서비스, 즉 웹을 통해 소프트웨어를 원격으로 사용할 수 있는 모델이라는 점에서 기존의 라이선스 모델과는 확연히 구분되며 보다 많은 장점을 가진다.

SaaS 는 통상적으로 Web 2.0 과 맞물려 일반 사용자를 대상으로 하는 SaaS 제공 업체로는 Google, Yahoo! 등이 있고, Enterprise 2.0 과 맞물려 기업 사용자를 대상으로 하는 SaaS 제공 업체로는 salesforce.com 가 대표적이다.

나. SaaS 구조

그림 2 는 SaaS 서비스 구조를 보여준다. 모든 소프트웨어는 서비스의 형태로 사용자에게 제공된다. SaaS Developer 는 소프트웨어 서비스를 Developer Platform 에서 개발한 후, SaaS Provider Platform 에 옮긴 다음 사용자의 접속을 기다린다. 사용자는 서비스 검색도구와 서비스 연동도구 등을 통하여 원하는 서비스들을 검색한 후, 연동하여 사용한다.



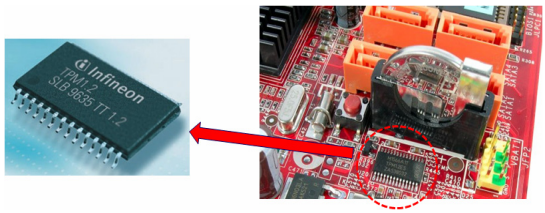
(그림 2) SaaS 모델의 서비스 구조

다. SaaS 현황

현재 국외 SaaS 시장에서는 Salesforce.com 등 온디맨드 소프트웨어 시장에서 고부가가치를 창출하는 독립적인 유통채널 기업이 등장하였고, 마이크로소프트, Google 등 웹 오피스 프로그램 서비스를 중심으로 하는 포탈형 서비스 기업도 등장하였다. 국내에서는 네이버와 씽크프리가 공동 개발한 웹 오피스인 싱크프리 오피스(Thinkfree Office)가 2007 년 9 월부터 온라인 서비스 형태로 제공되고 있으며 오픈 마루는 2006 년 3 월 스프링노트(Springnote)라는 웹 오피스를 출시하였다.

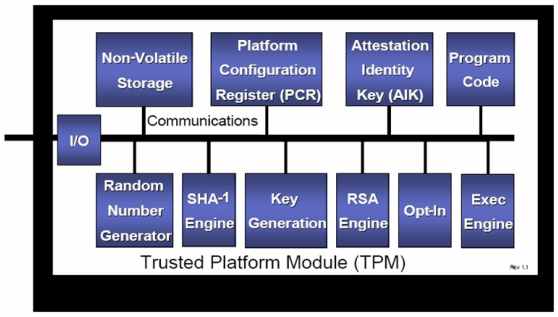
2.2 TPM

가. TPM 개요



(그림 3) TPM / 메인보드 상에서의 TPM

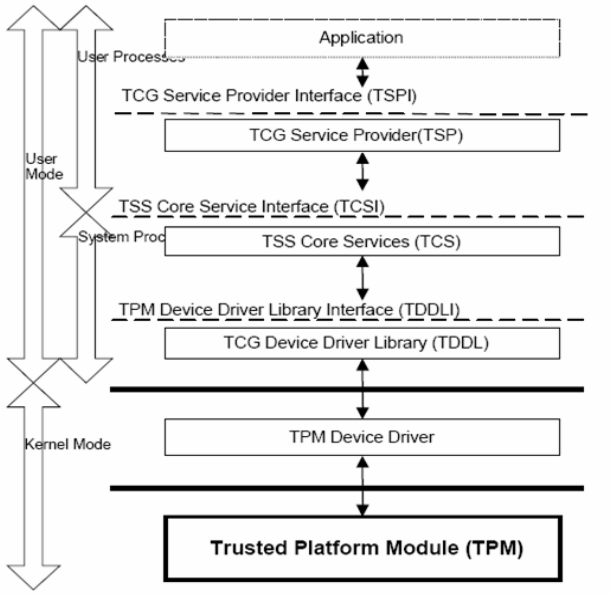
TPM(Trusted Platform Module)은 TCG(Trusted Computing Group)에 의해 제정된 산업 표준 규격을 기초로 한 보안칩(Security Chip)으로 마이크로 컨트롤러, 암호 엔진, 표준 입출력 인터페이스, 안전한 메모리를 갖추고 공개키, 디지털 인증서, 암복호, RNG(Random Number Generator), 인증, 보증, 민감 데이터 보호 기능을 제공한다[7]. 그림 3 은 TPM 칩과 메인보드 상에서의 TPM 칩을 나타낸다. 이러한 TPM 은 저전력, 고성능 프로세서 설계 기술을 요구하며, 칩 자체에 물리적인 공격에 대처하기 위한 센서와 내부 보안 구조로 되어 있어 내부에 저장된 보안 정보들의 누출이 현실적으로 불가능하도록 제작되어 있다. 그림 4 은 TPM 의 내부 구조를 나타낸다.



(그림 4) TPM 내부 구조

나. TPM 에 기반한 신뢰 플랫폼

TPM 을 기반으로 한 신뢰 플랫폼의 구조는 그림 5 과 같이 최하단에 TPM 칩이 있고, 이 TPM 과 관련된 인터페이스를 초기화하고 LPC 버스를 통해 TPM 과 데이터를 교환하는 하드웨어 기반 디바이스 드라이버인 TPM Device Driver(커널 모드)가 그 위에 존재한다. TPM Device Driver 의 상위 레벨에는 TSS 가 위치하게 된다.



(그림 5) TPM 에 기반한 신뢰 플랫폼의 구조

TSS(TCG Software Stack)는 TPM 을 기반으로 한 플랫폼 상에서 TPM 과 관련된 어플리케이션에게 TPM 기능 사용에 대한 단일 엔트리 포인트를 제공하고, TPM 에 대한 동기화된 엑세스를 제공하며, 명령어 스트림을 정확한 바이트 오더링으로 숨기고, TPM 리소스를 관리하는데 목적을 둔다. TSS 의 최하단의 TPM Device Library(TDDL)는 TPM 어플리케이션에 대하여 운영체제 독립적인 인터페이스를 제공하고 다양한 TSS 구현들이 어떠한 TPM 과도 정확히 통신할 수 있도록 해주는 역할을 한다. 그 상위 레벨의 TSS Core Services(TCS)는 일반 서비스들에 대한 인터페이스를 제공하고 여러 개의 TSP 가 있는 단일 플랫폼상에서도 TCS 는 모든 TSP 들을 정상적으로 호출할 수 있도록 한다. 마지막 TSS 의 최상위 레벨에는 TSS Service Provider(TSP)가 존재한다. TSP 는 어플리케이션과 동일한 프로세스 주소 공간에 존재하면서 TPM 에 대한 C 언어 인터페이스를 제공한다. 또한 어플리케이션과 TSP 리소스를 효과적으로 사용할 수 있도록 암호 서비스를 제공한다.

다. TPM/J

TPM/J[8]는 MIT 대학의 신뢰 컴퓨팅 프로젝트 연구로 개발되었으며, TPM 에 저 수준(low-level) 접근을 위한 Java 언어 기반 객체 지향 API 이다. TPM/J 는 TPM 관련 개발자들에게 좀 더 높은 편의성과 사용성을 제공하기 위해 유연한 객체 지향 API 를 제공하는데 그 목적을 두고 있으며, 이러한 의미에서 TCG 에서 제안한 TSS 구조를 모두 만족하지는 않는다.

TPM/J 는 저 수준 TPM 명령어를 Java 언어의 클래스로 추상화하여 사용자와 개발자에게 편의성을 제공하고 TPM 칩을 TPM Driver 라는 객체로 추상화함으로써 플랫폼 독립적인 TPM 어플리케이션을 개발 가능하게 하는 특징을 지니고 있다.

3. 설계 및 구현

3.1. 신뢰 컴퓨팅 기반 SaaS 모델 설계

그림 6 과 같이 SaaS 모델에서 SaaS Developer 는 서비스 소프트웨어를 Developer Platform 에서 개발한 후 SaaS Provider Platform 에 옮긴 다음 사용자의 접속을 기다린다. 사용자는 서비스 검색도구와 서비스 연동도구 등을 통하여 원하는 서비스들을 검색한 후 연동하여 사용한다.

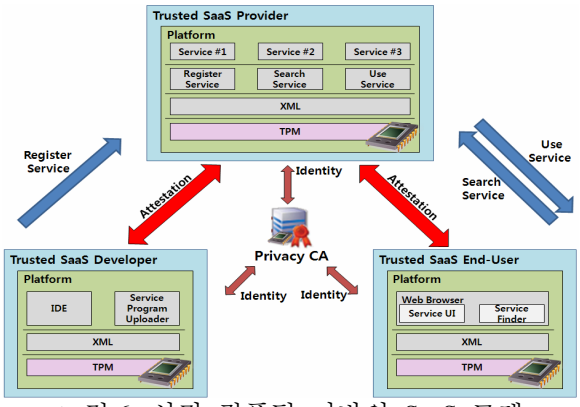


그림 6. 신뢰 컴퓨팅 기반의 SaaS 모델

각 플랫폼은 사용자의 신원을 확인하고 인증 받기 위해서 인증기관(Privacy CA: Privacy Certificate Authority)에게 자신의 TPM 정보를 전달하고 인증기관은 신원확인 요청을 한 플랫폼의 TPM 정보를 이용하여 생성한 보증서(Attestation Certificate)를 플랫폼에게 전달한다. 이 보증서를 가지고 각 액터(SaaS Provider, SaaS Developer, SaaS End-User)는 상대 액터의 플랫폼을 검증한다. 검증을 하기 위해서 플랫폼은 자신이 인증기관으로부터 받은 보증서와 TPM 이 서명한 PCR 값, SML(Stored Measurement Log)에 저장된 로그 값을 상대 플랫폼으로 전송한다. 이를 받은 플랫폼은 전송된 SML 의 로그 값으로부터 해쉬 값을 구하고 TPM 의 서명으로부터 PCR 값을 복원하여 서로 비교함으로써 플랫폼의 무결성을 검증한다.

3.2. 로컬 PC 레벨 무결성 검증 어플리케이션 구현

본 절에서는 앞에서 제시한 신뢰 컴퓨팅 기반의 SaaS 모델에서 기초가 되는 두 가지 프로그램을 구현한다. 구현에 있어서 OS 는 Microsoft 사의 Vista 를 사용하고 TPM 칩의 제어에 있어서 TSS 라이브러리는 TPM/J 를 사용한다.

가. 로컬 PC 레벨의 PCR 값 인증 프로그램

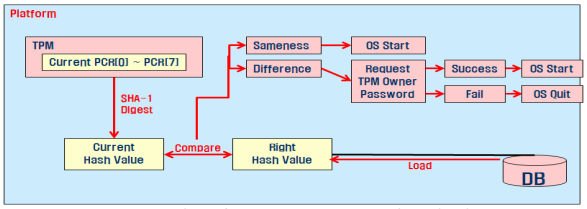


그림 7. PCR 값 인증 프로그램의 실행 흐름도

그림 7 과 같은 시퀀스를 갖는 프로그램은 사전에 올바른 플랫폼이라는 전제하에 PCR(0) ~ (7)까지, 부팅 과정에서 측정되는 PCR 들의 해쉬 값을 파일로 저장해둔다. 차후, 부팅과정에서 측정된 PCR 값과 사전에 저장해 둔 PCR 값의 해쉬 값을 비교하여 두 개의 PCR 값이 다르다면 현재 플랫폼에 변화가 있다는 점을 사용자에게 알리고 올바른 사용자임을 증명하는 루틴을 추가하여 플랫폼의 무결성을 재 검증할 수 있다.

나. 로컬 PC 레벨 어플리케이션 무결성 측정 프로그램

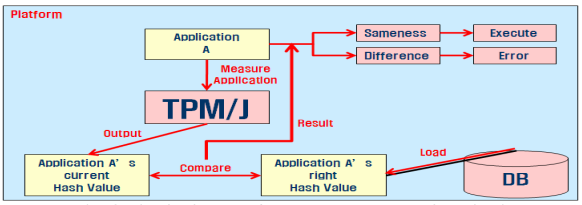


그림 8. 어플리케이션 인증 프로그램의 실행 흐름도

그림 8 과 같은 시퀀스를 갖는 프로그램은 OS 상에서 특정 어플리케이션(워드, 엑셀 등)의 실행 시, 해당 어플리케이션의 현재 해쉬 값을 구하고 이를 사전에 올바른 어플리케이션이라는 전제하에 저장해둔 해쉬 값과 비교하여 그 값이 같으면 어플리케이션을 실행하고 그렇지 않을 경우 에러메시지를 출력하면서 해당 어플리케이션을 종료하는 프로그램이다.

4. 성능 평가

먼저, 로컬 PC 레벨의 PCR 값 인증 프로그램에서는 하드웨어 구성과 BIOS 셋업을 변경하여 PCR 값을 변화시켰을 때, 사용자에게 별도의 패스워드 입력을 요청하는 과정이 발생하였다. 이 과정에서 유효하지 않은 패스워드 입력 시, OS 가 곧바로 종료됨을 확인할 수 있었다. 단, OS 로딩 단계에서가 아닌 OS 가 실행된 뒤, 값을 비교하였다는 단점이 있다. 하지만 이 같은 단점은 OS 제조사와의 협조를 통해서 해결할 수 있다.

어플리케이션 인증 프로그램에서는 실행될 어플리케이션의 설정 파일들을 바꾸었을 때, 그 해쉬 값의 차이로 인해 어플리케이션이 실행되지 않는 것을 확인할 수 있었다. 단, 해쉬 값을 구할 어플리케이션의 파일이 50MB 이하로 제한된다는 단점을 지니고 있다. 하지만 이는 어플리케이션 전체가 아닌, 몇몇의 핵심적인 파일만을 선택하여 그 해쉬 값을 구하는 방법을 선택하여 해결할 수 있다.

5. 결론

본 논문에서는 TPM(Trusted Platform Module)을 이용한 신뢰 컴퓨팅 기반 SaaS 모델을 설계하고, 설계된 SaaS 모델을 위한 로컬 PC 레벨 무결성 검증 어플리케이션을 구현하고 이를 평가하였다.

본 논문에서 제안한 설계 모델이 구현되고 널리 보급된다면 기존의 SaaS 시장은 신뢰성 있는 데이터 교환으로 인해 점차 확대될 것으로 예상되며, TPM 역시 그 보안성을 인증 받아 점차 보편화될 것으로 예상된다.

참고문헌

[1] Mark Turner, David Budgen, Pearl Brereton, "Turning Software into a Service", Keele University, Staffordshire, IEEE Computer Society, 2003.

[2] 문병주, " SaaS(Software as a Service) 동향", IITA 주간기술동향 통권 1306 호, 2007.7.25

[3] Mackinsey & SandHill Group, "Software 2006 Industry Report", 2006.

[4] 이상환, 김정윤, 전성익, " 신뢰 컴퓨팅기술 기반 SaaS 인증 및 과금 플랫폼 구조 설계," 한국정보처리학회, 추계학술발표대회, 제 14 권, 2007.11.

[5] S.W. Smith, " Trusted Computing Platforms: Design and Applications," Springer, 2005.

[6] Trusted Computing Group Website, http://www.trustedcomputinggroup.org/

[7] 김무섭, 신진아, 박영수, 전성익, "모바일 플랫폼용 공통보안핵심 모듈 기술," 정보보호학회지, 제 16 권, 제 3 호, 2006.6.

[8] TPM/J Website, http:// sourceforge.net/projects/tpmj/