신뢰 보안 모듈을 이용한 IoT 기기 간 원격 인증 방법에 관한 연구

한진희, 전용성
한국전자통신연구원 사이버보안연구본부 모바일보안연구실
e-mail : hanjh@etri.re.kr, ysjeon@etri.re.kr

A Study on the Remote Authentication Method between IoT Devices using a Trusted Security Module

Jin-Hee Han, YongSung Jeon
Mobile Security Research Section, Cyber Security Research Division, ETRI

요 약

IoT 환경에서 서로 다른 사양을 갖는 기기 간 통신에서의 보안 취약성, 사용자의 프라이버시 데이터 유출, 인가 받지 않은 기기나 사용자로 인한 기기 위·변조, 기기 오작동 등의 보안 위협 발생 가능성이 증가할 것이라는 예측과 더불어 다양한 보안 위협에 대응할 수 있는 보안 기술에 대한 관심이 높아지고 있다. 본 논문에서는 신뢰 보안 모듈과 클라우드 서버를 이용한 기기 간 원격 인증 및 기기 관리 방법에 대해 기술한다. 수 많은 기기가 인터넷으로 연결되어 운용되는 IoT 환경에서 신뢰 보안 모듈을 활용한 IoT 기기 간 원격 인증, 기기 보안 업데이트 및 안전한 기기 관리 기능 등을 통해 보다 안전하고 신뢰할 수 있는 IoT 서비스 제공이 가능해질 수 있을 것이다.

1. 서론

지능화된 사물들이 다양한 네트워크를 통해 연결되어 사람과 사물 또는 사물과 사물 간에 상호 소통하며 지능적인 서비스를 제공해주는 IoT (Internet of Things, 사물인터넷)는 최근 모바일, 클라우드, 빅데이터 기술 등과 융합하여 초 연결 사회를 이룰 수 있는 유망기술로 각광받고 있다. 하지만, IoT 서비스가 점차 확대되어 감에 따라 다양한 기기 간 통신, 이기종 네트워크 간 연동 시 기기 간 악성코드 전이 및 공격 위협 증가, 크로스 네트워크 기기로의 피해 확산 등 다양한 보안 위협에 대응할 수 있는 보안 기능의 필요성과 중요성이 부각되고 있는 추세이다[1].

하지만, 소프트웨어 기반 보안 방식은 조작 및 변조의 용이성으로 인해 다양한 보안 위협에 대응하기에는 역부족이라는 결론이 지배적이다. 이로 인해 소프트웨어 기반 보안 방식이 가지는 여러 취약점들을 보완할 수 있는 하드웨어 기반 보안 방식으로 PC, 노트북, 모바일 기기에 장착 되어 다양한 보안 기능을 제공해주는 TCG (Trusted Computing Group) 표준 신뢰 보안 모듈인 TPM (Trusted Platform Module), MTM (Mobile Trusted Module) 기반 하드웨어 보안 기술을 적용하여 기기의 정보유출 방지 및 보안성을 강화할 수 있는 방법들이 제안되었다[2][3].

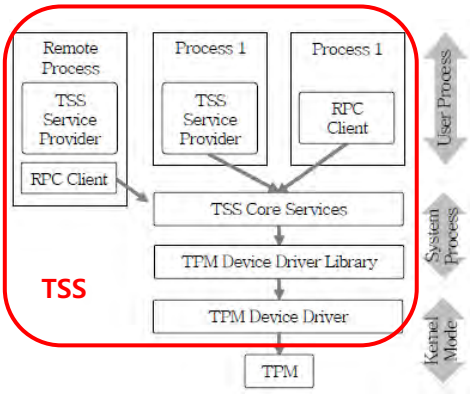
TPM 은 CPU 프로세서와는 달리 단순히 키 값이나 패스워드, 디지털 인증서 등을 저장할 수 있는 저장 공간을 제공함과 동시에 암호화 엔진을 제공한다[4]. TCG 는 PC 환경에 적합하도록 개발된 TPM 외에 모바일 단말에 적합한 MTM 도 제안하고 있는데, MTM 은 TPM 이 제공하는 보안 기능 중 일부 기능을 채용함과 동시에 모바일 환경에 필요한 다양한 보안 기능을 추가로 제공한다.

본 논문에서는 악성코드 탐지 및 해킹 차단, 사용자 인증을 비롯해 플랫폼 인증, 기기 인증, 데이터 보호, 안전한 키 관리 등의 보안 기능을 제공하는 TPM 혹은 MTM (이하 '신뢰 보안 모듈'이라 함)과 클라우드 서버를 활용한 IoT 기기 간 원격 인증 및 IoT 기기 관리 방법에 대해 자세히 기술한다.

이하 논문의 구성은 다음과 같다. 논문의 2 절에서는 TCG 의 신뢰 보안 모듈 기술에 대해 간략히 소개하고, 3 절에서는 신뢰 보안 모듈과 클라우드 서버를 활용한 IoT 기기 간 원격 인증을 위한 시스템 구성 및 구현 방법에 대해 상세히 설명한다. 마지막으로, 4 절에서는 향후 연구 계획과 함께 논문을 마무리 하고자 한다.

2. TCG 신뢰 보안 모듈

TCG 에서 제안한 신뢰 컴퓨팅 (Trusted Computing) 기술은 신뢰 보안 모듈과 TSS (TCG Software Stack) 및 분야별 응용 펌웨어 혹은 소프트웨어 라이브러리로 구성되며, 사용자 및 제조사 모두에게 신뢰 기반을 제공한다[5][6][7]. 신뢰 컴퓨팅 기술이란 컴퓨터가 당초 의도된 대로 동작할 수 있도록 신뢰성을 부과하는 기술로서, 하드웨어 기반의 보안 칩인 신뢰 보안

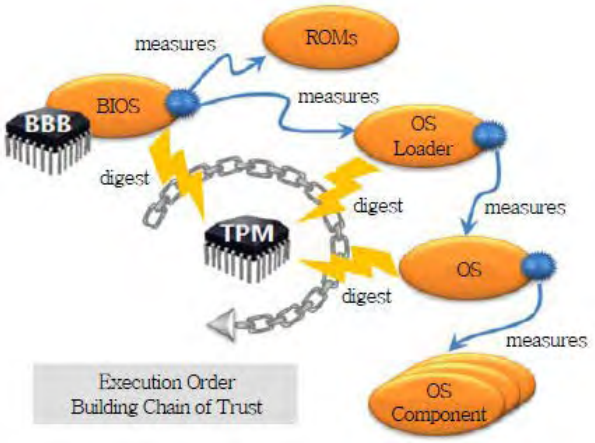


(그림 1) TPM(또는 MTM)과 TSS 구조

모듈을 모든 컴퓨팅 파워가 있는 기기들에 공통으로 적용하도록 하고, 이를 위한 소프트웨어를 개방형 표준으로 제공하고자 하는 기술이다.

(그림 1)은 신뢰 컴퓨팅 기술을 구성하는 신뢰 보안 모듈과 TSS 구조를 보여준다. 신뢰 컴퓨팅 기술의 핵심 구성 요소인 신뢰 보안 모듈은 tamper-proof 특성을 지니고 외부의 어떠한 공격에 대해서도 데이터, 키, 인증서 등을 안전하게 보호할 수 있는 저장 영역을 제공하며, 특히 키 저장 및 관리 기능에 보안성이 강화되어 있다. 또한, 비밀키를 외부로 유출하지 않고 암·복호 및 서명 검증 기능을 신뢰 보안 모듈 내부에서 수행하도록 설계되어 있으며, SRK (Storage Root Key) 기반 하에 안전 저장 영역을 계층적인 구조로 관리한다. 더불어, RTS (Root of Trust for Storage), RTM (Root of Trust for Measurement), RTR (Root of Trust for Reporting), RTV (Root of Trust for Verification) 기능을 통해 기기의 플랫폼 신뢰성을 설정하고, 플랫폼을 왜곡시킬 수 있는 외부 공격으로부터 플랫폼 무결성을 보장할 수 있다.

앞서 설명한 신뢰 보안 모듈의 RTS, RTM, RTR, RTV 기능을 이용하여 chain of trust 가 어떻게 이루어지는가를 (그림 2)에서 확인할 수 있다. (그림 2)에서 볼 수 있듯이 플랫폼을 구성하는 BBB (BIOS Boot Block)를 시작으로 해당 모듈의 무결성 값을 측정하고 검증한 후, 신뢰 보안 모듈에 검증이 완료된 측정값을 저장하고 모든 측정 데이터를 메모리에 기록하는 과정이 순차적으로 진행된다. 또한, 신뢰 보안 모듈은 통신하고자 하는 상대 플랫폼이 현재 신뢰할 수 있는 상태인지를 원격으로 검증 (Remote Attestation)할 수 있는 기능도 제공한다.



(그림 2) Chain of Trust

3. 신뢰 보안 모듈을 이용한 IoT 기기 간 원격 인증

온라인 공간에 흩어져있는 콘텐츠를 저장하여 통합 관리함으로써 언제 어디서나 다양한 기기를 통해 접근할 수 있는 환경을 제공해주는 클라우드 서비스는 기하급수적으로 콘텐츠가 증가하는 IoT 서비스 환경에 반드시 필요한 기술이다. 그러나, 클라우드 서비스는 기본적으로 네트워크에 연결되어 운영되기 때문에 서버나 기기, 네트워크, 데이터 등에 대한 인증 및 보안 기능이 클라우드 서버를 활용한 다양한 서비스에 적용될 수 있도록 해야 한다. 본 논문에서 제안하는 신뢰 보안 모듈과 클라우드 서버를 이용한 기기 간 원격 인증 및 기기 관리 방법은 이러한 다양한 기기와 장치들간의 상호 연결, 통신에 기반한 IoT 특성을 고려한 구조를 갖는다.

(그림 3)은 클라우드 서버와 게이트웨이 및 다양한 기기들로 구성된 IoT 서비스 환경에서 클라우드 서버와 게이트웨이에 신뢰 보안 모듈을 탑재하여 기기 간 원격 인증 및 기기 관리를 제공하는 과정을 보여준다.

(그림 3) 신뢰 보안 모듈을 이용한 IoT 기기 간 원격 인증

일례로, 게이트웨이 1 의 기기 1 이 게이트웨이 2 의 기기 1 과 통신을 하고자 할 경우, 게이트웨이 1 이 기기 1 에 대한 인증 및 무결성 정보를 정상적으로 확인하고 클라우드 서버의 신뢰 보안 모듈에 저장된 게이트웨이 2 의 인증 및 무결성 정보를 얻어 게이트웨이 2 가 신뢰할 수 있는 안전한 상태인지를 확인한다. 만일, 게이트웨이 2 의 상태가 안전하다면 게이트웨이 1 은 게이트웨이 2 의 기기 1 과 통신을 허락한다. 만일, 게이트웨이 1 또는 게이트웨이 2 가 신뢰할 수 없는 상태이거나 게이트웨이 2 의 기기 1 이 신뢰할 수 없는 상태일 경우 상호 통신은 이루어지지 않는다.

(그림 3)에서 보는 바와 같이, 게이트웨이와 클라우

드 서버에 탑재된 신뢰 보안 모듈은 기기의 인증, 무결성 검증, 업데이트 등과 관련된 기능을 수행하고, 결과 값을 안전하게 저장하고 관리하는 역할을 담당한다. 게이트웨이에 탑재된 신뢰 보안 모듈은 게이트웨이에 연결되어 있는 IoT 기기들의 인증, 무결성 검증, 업데이트 등의 기능을 담당하며, 클라우드 서버에 탑재된 신뢰 보안 모듈은 게이트웨이들의 인증, 무결성 검증, 업데이트 등의 기능을 처리한다.

신뢰 보안 모듈은 특정 메시지 형식에 맞춰 외부와 통신을 하기 때문에 이를 위해 게이트웨이나 클라우드 서버 내에 신뢰 보안 모듈과의 통신을 위한 메시지 생성 및 처리 모듈이 추가되어야 하며, 기기 인증 및 플랫폼 무결성 검증 기능을 수행하기 위해 기기 인증 모듈과 플랫폼 무결성 검증 모듈이 게이트웨이, 클라우드 서버 및 신뢰 보안 모듈에 각각 구현되어 운영되어야 한다.

(그림 4)와 (그림 5)는 IoT 기기 간 원격 인증을 위해 게이트웨이와 클라우드 서버 및 신뢰 보안 모듈에 구현되어야 할 내부 기능 구성도를 보여준다.

(그림 4)와 같이 게이트웨이와 게이트웨이에 탑재되는 신뢰 보안 모듈은 크게 기기 인증, 인증 정보 저장, 인증 정보 전송, 기기 업데이트, 인증 결과 승인, 통신 기능 등을 제공한다. 게이트웨이와 신뢰 보안 모듈에서 수행되는 각각의 기능은 다음과 같다. 기기 인증을 수행한 후, 인증 정보 저장부에 기기 번호를 토대로 수집된 기기 인증 정보를 안전하게 저장한다. 인증 정보 전송부는 수집된 기기 인증 정보를 클라우드 서버로 전송하며, 업데이트부는 클라우드 서버로부터 전송된 소프트웨어 업데이트 파일을 검증한 후 해당 기기를 업데이트한다. 통신 요청부는 다른 기기와의 통신 연결이 필요한 경우, 클라우드 서버에 해당 기기와의 상호 연결을 요청하며 인증 결과 수락부는 클라우드 서버로부터 연결 요청 대상으로 지목된 게이트웨이와 기기의 인증 및 무결성 검사 결과를 수신하는 역할을 담당한다. 마지막으로, 통신부는 인증 결과 수락부에서 수신한 연결 요청 대상의 인증 정보 및 무결성 정보에 따라 상호 통신을 허가하거나 차단하는 기능을 수행한다. 앞서 설명한 내용 중 기기 인증, 기기 인증 정보 저장 등 보안성이 요구되는 기능은 신뢰 보안 모듈이 전담한다.

(그림 4) 게이트웨이에 탑재된 신뢰 보안 모듈 내부 구성도

반면, 클라우드 서버와 클라우드 서버에 탑재되는 신뢰 보안 모듈의 내부 기능은 (그림 5)와 같이 구성

(그림 5) 클라우드 서버에 탑재된 신뢰 보안 모듈 내부 구성도

된다. 구성 요소로는 통신 요청 수신, 게이트웨이 검사, 기기 검사, 통신 연결 중계, 정보 저장, 기기 상태 업데이트, 보고 기능 등이 존재한다. 통신 요청 수신부는 예를 들어 게이트웨이 1 로부터 게이트웨이 2 와 연결된 기기 또는 게이트웨이 2 로부터 게이트웨이 1 과 연결된 기기와의 통신 연결 요청을 수신한다. 게이트웨이 검사부는 통신 연결을 요청한 게이트웨이 1 및 게이트웨이 2 에 대한 인증 및 무결성 정보를 검사하고, 기기 검사부는 통신 연결을 요청한 게이트웨이와 연결된 기기에 대한 인증 및 무결성 정보를 검사한다. 모든 검사 결과는 보고부를 통해 해당 게이트웨이로 전송된다. 또한, 정보 저장부는 게이트웨이, 게이트웨이에 연결된 기기의 인증 및 무결성 정보를 저장하며, 업데이트 수행부는 게이트웨이 및 게이트웨이와 연결된 기기에 대한 인증, 무결성, 소프트웨어 업데이트 상태, 연결 정보 등에 변경사항이 발생한 경우 해당 정보를 업데이트한다. 마지막으로, 통신 연결 중계부는 게이트웨이 및 기기 검사 결과를 토대로 게이트웨이간의 통신 연결을 허가하거나 차단하는 기능을 수행한다. 클라우드 서버에 탑재된 신뢰 보안 모듈 역시 게이트웨이 인증, 기기 인증, 기기 인증 정보 저장 등 보안성이 요구되는 기능을 전담한다.

또한, 게이트웨이와 각 게이트웨이에 연결된 기기들의 소프트웨어 업데이트 즉, 게이트웨이 개발사 또는 기기 개발사에서 해당 기기에 대한 소프트웨어 업데이트가 필요한 경우, 클라우드 서버와 개발사의 서버간에 상호 인증을 수행한 후 개발사에서 클라우드 서버에 해당 기기의 소프트웨어 업데이트 파일을 전송하여 저장한다. 이때 전송되는 소프트웨어 업데이트 파일 내용은 기밀성 유지를 위해 암호화되거나 서버간 신뢰 통신 채널을 통해 안전하게 전송한다.

소프트웨어 업데이트 파일 전송이 모두 완료되면 클라우드 서버는 해당 기기가 업데이트 될 시점임을 신뢰 보안 모듈에 기록하고, 소프트웨어 업데이트가 필요한 해당 기기에게 업데이트 파일을 안전하게 전송한다.

4. 결론

최근 다양하고 새로운 IoT 서비스가 등장하면서 여러 가지 사양과 특성을 갖는 수 많은 기기 간의 연결

과 통신의 증가가 예상되고 있다. 이러한 IoT 서비스 환경의 특성으로 인해 발생 가능한 다양한 보안 위협에 대응하기 위해 안전한 서비스 환경 구축 및 서비스의 보안성 강화는 반드시 수반되어야 한다. 본 논문은 신뢰 보안 모듈과 클라우드 서버를 이용한 IoT 기기 간 원격 인증 방법과 기기 관리 방법을 제안하고, 기기 간 원격 인증을 제공하기 위해 게이트웨이 및 클라우드 서버, 신뢰 보안 모듈에 구현되어야 할 내부 기능과 적용 방안에 대해 상세히 기술하였다

향후, 신뢰 보안 모듈과 연동이 가능한 IoT 기기와 게이트웨이와의 연계 방법, 신뢰 보안 모듈을 활용하여 다양한 기기 특성 및 사양에 따라 보안 등급을 부여하고 운용할 수 있는 방안에 대한 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

이 논문은 2015 년도 정부(미래창조과학부)의 재원으로 정보통신기술연구진흥센터의 지원을 받아 수행된 연구임 (No.R-20150518-001267, 스마트 경량 IoT 기기용 운영체제 보안 핵심 기술 개발)

참고문헌

[1] S. Sicari, A. Rizzardi, L.A. Grieco, and L.A. Grieco, “Security, privacy and trust in Internet of Things: The road ahead,” ELSEVIER, Computer Networks, vol. 76, January 2015, pp. 146–164

[2] S. Choi, J. Han, J. Lee, J. Kim, S. Jun, “Implementation of a TCG-based trusted computing in mobile device”, TrustBus 2008, LNCS vol. 5185, pp. 18-27

[3] R. Sailer, X. Zhang, T. Jaeger, L. Doorn, “Design and implementation of a TCG-based integrity measurement architecture”, 13th USENIX Security Symposium, 2004, pp. 223-238

[4] Siani Pearson, Trusted Computing Platforms, Prentice Hall PTR, 2000

[5] TCG: TCG Specification Architecture Overview, Revision 1.4, August 2007, http://www.trustedcomputinggroup.org

[6] TCG: TCG Mobile Reference Architecture, Ver.1.0. Revision 1, June 2007, http://www.trustedcomputinggroup.org

[7] TCG: TCG Software Stack. Specification, Ver.1.2, March 2007, http://www.trustedcomputinggroup.org