IoT 소프트웨어 위변조방지를 위한 Open Titan Chip 기반 Remote Attestation

이해성, 정재훈, 신동우*, 이상한*

성균관대학교 소프트웨어학과, *ETRI부설연구소

{haesung0908, pauljeong}@skku.edu, {dwshin, freewill71}@nsr.re.kr

Open Titan Chip-Based Remote Attestation for IoT Software Forgery Prevention

Haesung Lee, Jaehoon Jeong, Dongwoo Shin*, Sanghan Lee*

Department of Computer Science and Engineering at Sungkyunkwan University,
*The Attachment Institute of ETRI

요 약

최근 사물인터넷(IoT)의 규모가 증가함에 따라 기존보다 넓어질 연결성에 대한 기대로 인해 IoT는 큰 주목을 받고 있다. 이러한 IoT의 등장에 따라 IoT 디바이스 종단 간의 인증, 인가 및 보안 통신의 중요성이 역시 부각되고 있지만, 기존의 보안 체계는 비교적 고성능의 컴퓨팅 노드를 위하여 설계돼 있어 메모리, 연산 능력 등의 자원이 제약되는 IoT에는 적합하지 않다. 본 논문은 보안 통신을 위해 요구되는 암호화 키나 암호화 연산을 처리할 수 없는 제약적인 IoT 디바이스를 위해 하드웨어 보안 칩인 Open Titan Chip을 활용하여 관리자 시스템을 통해 IoT 디바이스의 펌웨어 및 소프트웨어의 위변조를 모니터링하는 Remote Attestation을 제안한다.

Ⅰ. 서 론

최근 IoT 다양한 디바이스들이 등장하고 있으며, 가트너에서는 2020년 IoT 기기의 수가 204억대에 이를 것으로 전망하고 있다[1]. 국내 IoT는 Smart Home, Smart City, Smart Campus, Smart Road 등의 다양한 분야로 확산될 것으로 예상된다. 이렇듯 IoT 기술은 최적화된 환경을 제공하여 편리함과 효율성 증대라는 장점이 있지만, 신뢰성 및 제어와 정보 무결성 그리고 해킹 및 사생활 침해 등과 같은 피해 때문에 보안에 관한 중요성이 대두되고 있다. 자원 제약적인 IoT 디바이스 같은 경우, 메모리 및 연산 능력 등의 자원 부족으로 인하여 보안 통신을 위해 요구되는 암호화 키(Key)나 암호화 연산이 IoT에서 처리하기에는 큰 부담이다. 따라서 본 논문에서는 IoT의 소프트웨어 위변조 방지하기 위해 하드웨어 보안 칩인 Open Titan Chip을 활용하여 검증된 관리자 시스템을 통해 IoT 디바이스의 펌웨어(Firmware, FW) 및 소프트웨어(Software, SW)의 위변조를 모니터링하여 위변조를 방지하는 Remote Attestation을 제안한다. 제시하는 방안은 Open Titan을 통해 Remote Attestation 간 사용되는 정보를 안전하게 보호하고, 외부의 관리자 시스템과 IoT 디바이스 간의 안전한 데이터 전송을 한다.

Ⅱ. 관련 연구

Ⅱ-1. HSM

HSM(Hardware Security Module)은 암호화 키를 생성하고, 저장하는 역할을 하는 전용 장치로 암호화 키를 필요로 하는 다양한 애플리케이션이 있을 경우에 관련 키 생성 및 저장을 애플리케이션에서 하는 것이 아니라 전용 장치에서 한다[2]. HSM에 들어 있는 정보는 원천적으로 외부 복사 및 재생성이 되지 않는다.

HSM은 모바일 머니 지불 결재 보안을 위해 그리고 스마트폰을 통해 이루어지는 가족 은행 거래 관련 보안을 위해 사용된다. 하지만 암·복호 연산 수행을 위해 HSM으로 데이터, 명령어를 전송하고 처리된 결과를 받는 데 따르는 I/O로 인한 성능 저하는 자원이 제약된 IoT 디바이스에서는 큰 문제가 된다.

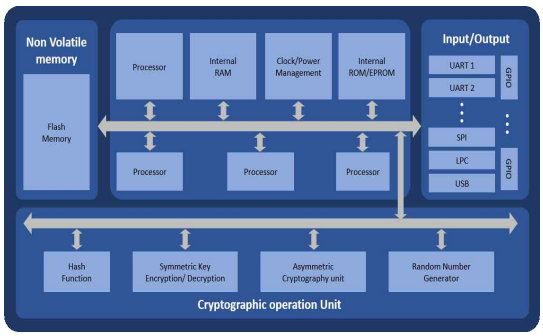

그림 1. HSM의 구조[2]

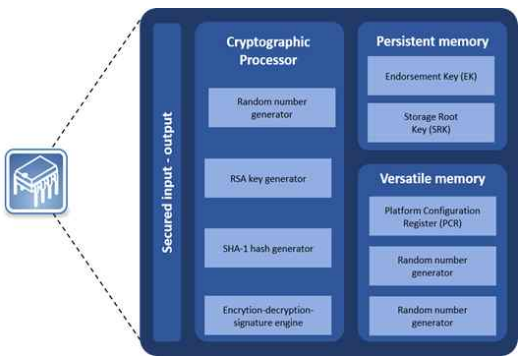

그림 2. TPM의 구조[3]

Ⅱ-2. TPM

TPM(Trusted Platform Module)은 암호화 작업을 수행하도록 설계된 암호화 프로세서이다[3]. 일반적으로 소프트웨어만으로 운영되는 보안 기

술은 다양한 보안 공격에 취약하므로 이러한 문제를 해결하고자 트러스티드 컴퓨팅 그룹(Trusted Computing Group, TCG)은 암호화 키 관리와 암호화 처리가 하드웨어 보안 칩 내부에서만 동작하도록 칩 표준 규격을 제시하였다. TPM이 사용되는 곳은 HSM과 유사하다. 하지만, 암호화 작업을 수행하는 TPM은 단일 플랫폼 내의 멀티 유저 환경에서 내부 공격자가 TPM으로 위장하는 공격에 취약하다고 밝혀졌다.

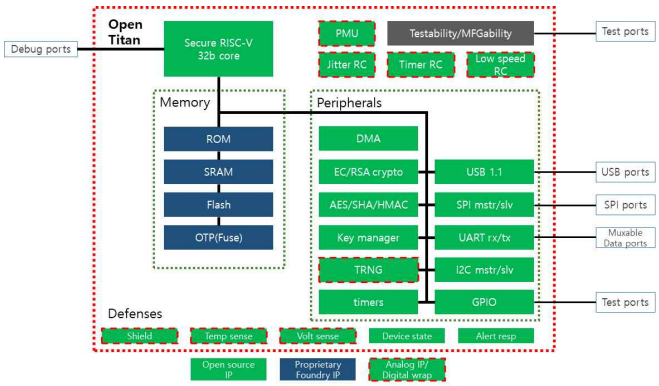

그림 3. IoT 보안을 위한 Open Titan Chip의 아키텍처

Ⅲ. 본론

기존에 소프트웨어 위변조를 위해 선행 연구된 HSM, TPM은 자원제약형 IoT 디바이스에 사용하기에는 무거울뿐더러 많은 취약점들을 보여주고 있다. 그림 3은 Open Titan의 구조로 IoT FW/SW 위변조방지를 위한 보안시스템 아키텍처를 보여준다. Open Titan Chip을 이용한 IoT 보안시스템은 RoT(Root of Trust) 기반의 Secure Booting을 통해 Remote Attestation을 수행할 수 있다[4]. Titan Chip은 제조사 독립적인 RoT를 보장하여 안전한 클라우드 시스템 운용이 실증되었으므로 IoT 디바이스를 위해 경량화된 Open Titan Chip은 IoT 보안을 위해 적합할 것으로 예상된다. Open Tian Chip을 IoT 디바이스 HW에 부착하여, IoT 디바이스의 BIOS 같은 FW와 운영체제 같은 시스템 SW에게 RoT를 제공하여, 서명, 인증, 암호화를 효과적으로 지원할 수 있다. 이러한 Open Tian Chip은 RoT를 저장한 메모리를 완벽히 보호하므로 안전한 부팅을 보장하여 신뢰성이 보장된 RoT를 제공함으로써 Remote Attestation을 완벽히 구현할 수 있다. 반면에 기존의 TPM은 RoT를 저장한 메모리를 완벽히 보호할 수 없으므로 신뢰성이 보장된 RoT를 제공하기 어렵다. 본 논문의IoT Remote Attestation은 IoT 디바이스의 FW/SW가 위변조되었는지, 사용자의 원하는 정책 또는 의도대로 잘 동작하고 있는지 원격에서 검사한다[3]. 본 논문은 [4]에서 제안한 Remote Attestation Framework를 기반으로 그림 4와 같이 IoT Remote Attestation Framework를 제안한다. 원격 검증절차는 다음과 같은 순서를 가지고 있다.

(1) IoT 디바이스 사용자(User)는 자신의 ID와 Identity Key를 통해 Attestation 하고자 하는 IoT 디바이스의 공개된 RoT 정보를 Trusted Third Party에 요청해서 수신함.

(2) 사용자는 IoT 디바이스와 신뢰된 통신 채널(Trusted Channel)을 셋업하기 위해 IoT 디바이스와 핸드세이킹(Handshaking)을 수행함.

(3) IoT 디바이스는 Trusted Third Party로부터 User의 공개된 RoT 정보를 수신하여 핸드세이킹에 응답함.

(4) 사용자는 IoT 디바이스에게 자신이 원하는 Attestation에 관련된 설정(Configuration) 또는 정책(Policy)을 포함하는 Configuration Request를 IoT 디바이스에게 전달함. IoT 디바이스는 사용자의 요청한 설정 또는 정책을 자신의 시스템에 반영함. IoT 디바이스는 사용자에게 Configuration Response를 송신함.

(5) 사용자는 Attestation을 위한 Report Request를 IoT 디바이스에게 송신하며, IoT 디바이스는 요청된 FW/SW 상태와 Task 수행 상황을 포함한 Report Response를 사용자에게 송신함. 사용자는 수신한 Report Response에 대해 IoT 디바이스의 Public Key로 검증하고, 유효한 Report Response에 대해서는 FW/SW가 위변조되었는지 또는 원하는 Task가 제대로 수행되고 있는지 확인함.

사용자는 원격 증명(Remote Attestation)을 위해 Nonce를 포함한 Report Request를 자신의 Private Key로 전자 서명하여 IoT 디바이스에게 송신한다. IoT 디바이스는 요청받은 Report Request를 사용자의 Public Key로 검증하고, 유효한 Report Request이면 송신 받은 Nonce를 포함하여 자신의 Private Key로 전자 서명하여 사용자에게 송부한다. Nonce는 사용하는 이유는 Replay Attack을 막기 위해서이다.

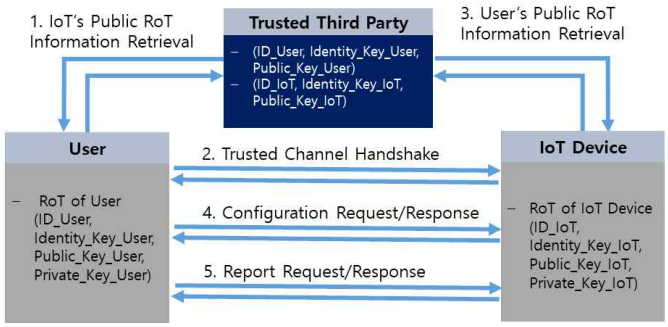

그림 4. Open Titan Chip 기반 IoT Remote Attestation

Ⅳ. 결론

본 논문에서는 자원 제약적인 IoT 디바이스의 FW/SW 위변조 모니터링 및 방지 방안을 제시하였다. 또한 본 논문은 Open Titan Chip 기반 Remote Attestation의 절차에 관해서 설명하였다. 제시하는 방안은 IoT에서 SW로만으로 자체 시스템의 FW/SW 위변조를 방지하기 어렵다. IoT 디바이스는 보안서비스 하기에는 메모리, 연산 능력 등의 자원 측면에서 한계가 있기 때문에 Open Titan을 IoT에 장착하여 인증된 관리자 시스템을 통해 IoT 디바이스의 원격 검증을 통해 FW/SW 위변조를 방지한다. 향후 연구에서는 본 논문에서 제시한 방안을 기반으로 하여 IoT 디바이스 Remote Attestation을 위한 원격 검증 시스템을 연구 및 개발을 진행할 예정이다.

ACKNOWLEDGMENTS

본 연구는 ETRI부설연구소의 자원제약형 IoT 장치를 위한 소프트웨어 위변조 방지기술 연구(2019-128)과제로 수행된 연구결과임. 또한 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업(IITP-2019- 2017-0-01633)의 연구결과로 수행되었음.

참 고 문 헌

[1] Gartner, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019", 2018.

[2] FORGEBox, "Hardware Security Module", http://www.forgebox.eu/fb/preview_course.php?course_id=182

[3] Musings, "TPM Architecture", https://blog.fpmurphy.com/2016/02/accessing-tpm-functionality-from-uefi-shell-part-1.html

[4] Pastor, D. Lopez, and A. Shaw, "Remote Attestation Procedures for Network Security Functions (NSFs) through the I2NSF Security Controller", draft-pastor-i2nsf-nsf-remote-attestation-07, Feb. 2019.