신뢰성 컴퓨팅 기반의 부팅 기술 분석을 통한 시큐어 부트로더 보안 요구사항 도출

국주희[O1] 이성기[2] 강태인[2] 김훈규[2] 최대선[3†] 박기웅[4†]
[1]세종대학교 시스템보안연구실
[2]국방과학연구소
[3]공주대학교 의료정보학과
[4]세종대학교 정보보호학과
soupjuhui@gmail.com, seongkeel@add.re.kr, tanekang@add.re.kr, hunk@add.re.kr,
sunchoi@kongju.ac.kr, woongbak@sejong.ac.kr

Security Requirements of Secure Bootloader through Trusted Computing-based Boot Technology Analysis

Ju-Hee Kook[O1] SeongKee Lee[2] Tae In Kang[2] Hoon Kyu Kim[2] Dae-seon Choi[3†] Ki-Woong Park[4†]
[1]Sejong Univ. Syscore Lab
[2]Agency for Defense Development
[3]Kongju National Univ. Dept. of Medical Information
[4]Sejong Univ. Dept. of Computer and Information Security

요 약

최근 드론의 활용 범위가 군사용, 농업용, 건설용 등으로 넓어짐에 따라 다양한 분야에서 주목을 받고 있다. 특히 군사 부문에 있어서 정찰용 목적을 넘어 무기를 탑재한 공격 수단으로 활용되고 있다. 작전에 활용되는 군사용 드론의 경우, 군사 기밀이 드론 내 컴퓨팅 시스템에 저장될 수 있기 때문에 드론에 대한 물리적 보안 뿐 아니라 시스템 소프트웨어에 대한 보안이 중요한 문제로 부각되고 있다. 예를 들어, 작전에 사용되는 군사용 드론에 위/변조되거나 취약점이 내재된 운영체제가 탑재되고 부팅될 경우, 기존 운영체제의 보안 기법이 무력화 될 수 있으며, 시스템 소프트웨어의 취약점을 이용한 드론의 제어권 탈취가 가능하기 때문에 드론 시스템에 탑재되어 실행될 부팅 단계별 실행 코드의 무결성 검증 기법이 필요하다. 본 논문에서는 부팅 프로세스의 무결성을 보장하기 위한 신뢰성 컴퓨팅 기반의 시큐어 부팅 기술과 군사 무기체계 분야에서 활용되고 있는 화이트리스트 기반의 시큐어 부팅 기술을 보안관점에서 비교 분석하여 이를 바탕으로 시큐어 부트로더 보안 요구사항을 도출한다.

1. 서 론

최근 군사용 드론이 정찰 및 감시용 목적을 넘어 무기체계 드론으로 활용되고 있다. 부팅 프로세스와 시스템 소프트웨어의 취약점을 통해 작전에 사용되는 드론의 제어권이 탈취 당했을 경우, 비행 정보가 조작되거나 군사용 드론 운영 시스템 정보 및 군사 기밀이 누출될 수 있어 군용 드론의 보안 중요성이 대두되고 있다.

특히 운영체제 부팅 이전 환경의 공격 기법은 모든 운영체제의 보안 기법을 우회할 수 있기 때문에 안전한 부팅 기법과 관련된 부팅 이전 보안이 주목을 받고 있다. 안전한 부팅이 보장되지 않으면 부트로더, 커널, 운영체제, 어플리케이션에 이르기까지 시스템의 위/변조와 관련된 다양한 보안 문제를 야기할 수 있다.[1] 따라서 기존의 부팅 단계마다 실행할 코드의 무결성을 측정하고 전체 시스템이 정상적인 부팅 프로세스를 거쳐 부팅되었음을 보장해야 한다.

부팅 프로세스의 무결성 보장을 위해 TCG(Trusted Computing Group)에서 부팅 단계별 하드웨어의 변화를 모두 감지할 수 있는 하드웨어 칩 기반의 암호화 처리 모듈이 개발되었다. T2080 프로세서의 경우, 부팅 프로세스의 무결성을 제공할 뿐만 아니라 실시간 무결성 검증 기능을 제공하며 비인가 사용자의 디버그 또는 JTAG 접근 차단 기능을 제공함으로써[2] 무기 체계 시스템에서 주목을 받고 있다. 따라서 본 논문에서는 TPM과 T2080 프로세서가 제공하는 부팅 프로세스를 보안 관점에서 비교해보고, 이를 바탕으로 보안 요구사항을 도출하고자 한다.

본 논문의 구성은 2장에서 컴퓨터 시스템의 부팅 프로세스와 TPM 및 T2080 프로세서를 사용한 시큐어 부팅 프로세스에 대해 소개하고, 3장에서는 TPM과 T2080 프로세서가 제공하는 시큐어 부팅 프로세스를 보안 관점에서 비교하여 서술한다. 4장에서는 결론을 제시한다.

---

† 교신저자: 최대선 (공주대학교 의료정보학과 교수), 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 한국연구재단 지원사업(2016R1A4A1011761) 및 국방과학연구소에서 수행중인 무기체계용 고신뢰 내장형 실시간 보안 OS 기술 개발과제(UD180001ED)의 지원으로 수행되었음

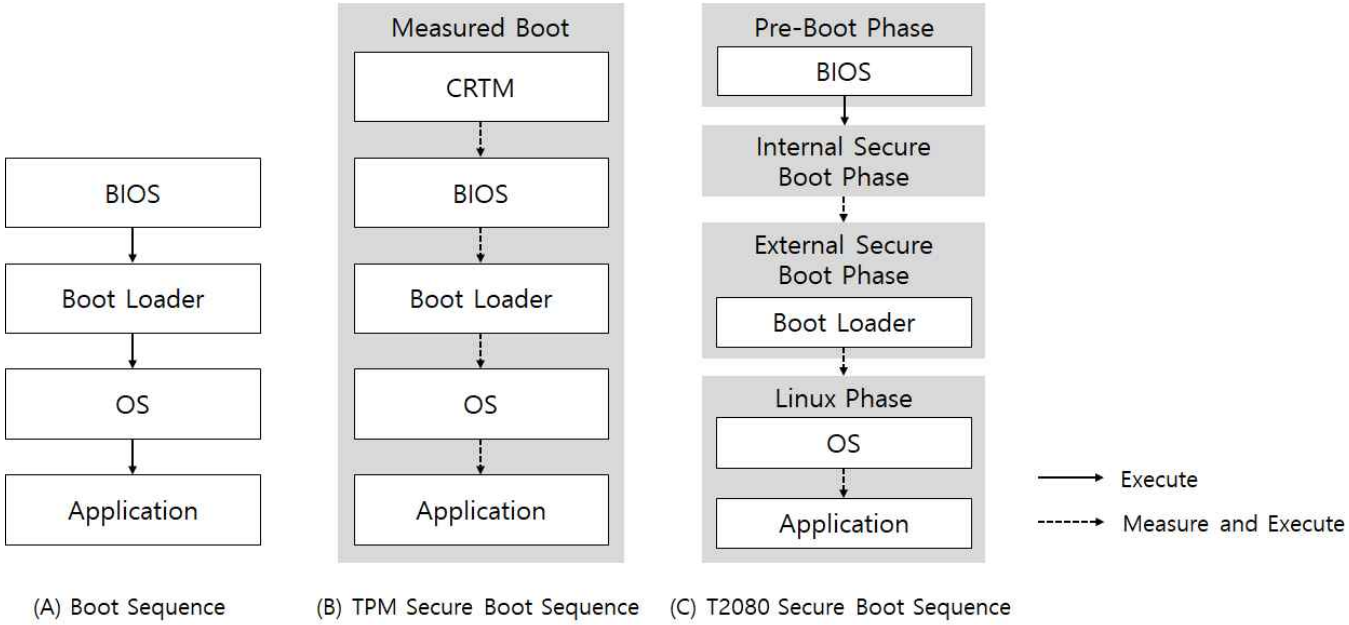

그림 1 부팅 프로세스 비교

2. 배경 지식

2.1 부팅 프로세스

부팅 프로세스의 세부적인 내용은 시스템마다 다르지만 공통적인 단계로 구분할 수 있다.

시스템에 전원이 공급되면 CPU가 메인보드의 ROM에 있는 BIOS(Basic Input Output System) 프로그램을 실행한다. 시스템에 문제가 있는지 확인하는 POST(Power On Self Test) 과정이 완료되면 디스크의 첫 번째 섹터에 존재하는 MBR(Master Boot Record) 코드를 실행한다. 부팅 가능한 파티션의 첫 번째 섹터에서 VBR(Volume Boot Record)를 찾고, VBR에서 사용자가 원하는 운영체제의 커널을 메모리에 적재하면 해당 운영체제가 실행된다.

2.2 TPM

TPM(Trusted Platform Module)은 신뢰할 수 있는 컴퓨팅 플랫폼을 제공하기 위해 TCG에서 개발한 하드웨어 칩 기반의 암호화 처리 모듈로 RSA와 SHA-1과 같은 암호화 엔진, 시스템의 무결성 보장 등의 기능을 수행한다.

PCR(Platform Configuration Register)은 플랫폼의 상태 값을 저장하기 위해 존재하는 160비트 레지스터[3]로 부팅 프로세스에 필요한 BIOS, 운영 체제 또는 응용 프로그램 등의 모든 시스템 정보에 대한 해시 값을 저장한다.[4] 데이터에 추가나 삭제로 인한 변화가 있을 때, 기존의 PCR 값과 결합하는 연산을 통해 누적 해시 형태로 저장하여 신뢰체인을 형성하기 때문에 플랫폼의 무결성을 검증하는데 사용될 수 있다.

TPM은 시스템 전원이 켜지면 BIOS가 실행되기 전부터 CRTM(Core Trust for Measurement)에서 SHA-1 해시 알고리즘을 기반으로 자체 무결성을 먼저 측정한다. 그런 다음 BIOS를 측정하고 PCR에 저장된 해시값과 비교하여 무결성을 검증한다. 마찬가지로 각 부팅 프로세스는 위와 같이 PCR에 저장된 해시값과 비교하여 무결성이 검증된 경우에만 실행한다. 무결성을 측정하여 신뢰 체인(Chain of Trust)을 구성하기 때문에 악의적인 사용자가 다른 운영체제를 부팅하거나 운영체제를 손상시키는 경우, PCR 값이 달라지므로 부팅 프로세스가 중단된다.[5]

2.3 T2080 프로세서

T2080 프로세서[6][7]는 시스템 위/변조 위협을 방어하기 위한 많은 매커니즘을 제공한다. 코드 실행 시 기록된 디지털 서명을 복호화하여 추출한 해시값과 실행 환경 코드의 해시값을 비교해 무결성을 검증하는 Code Signing 기술을 사용한다. 부팅 과정에서 T2080 프로세서의 인증을 우선적으로 실행하여 시스템 코드의 디지털 서명을 통해 위/변조를 검증한다. 따라서 무단 수정을 감지할 경우, 해당 코드가 부팅되지 않도록 부팅 프로세스를 중단한다.

T2080 프로세서에서 사용되는 E6500 코어는 시큐어 부트를 위한 기술을 제공한다. Internal Boot ROM의 외부 코드가 안전하게 실행되고 있는지 검증하며, No execute Bit(X-bit)를 사용해 특정 메모리 페이지의 실행을 사전에 차단하여 메모리 침범 공격을 사전에 예방한다. E6500 코어를 가상화하며 페이지 테이블 항목의 변조와 같은 중요한 보안 구성을 수정하려는 모든 게스트 운영체제의 시도를 차단하는 Embedded Hypervisor를 제공한다.

전원이 켜지면 시큐어 부팅이 필요한지 여부를 확인하고 외부 마스터(PCI Express, Serial Rapid IO)가 PAMU(Peripheral Access Management Units)에 의해 차단되었는지 확인하는 Pre-Boot 단계를 수행한다. 외부 마스터가 차단되면 Internal Secure Boot Phase 단계에서 Internal Boot ROM 명령어 실행을 통해, 유효성이 검증된 공개 키로 서명 유효성 검사를 수행하여 U-Boot 코드에 대한 디지털 서명을 검증한다. External Secure Boot

단계에서는 Trusted U-Boot가 실행되어 실제 메모리 매핑, Queue Manager 및 Boot Script 파일을 메인 메모리로 로드하는 등의 일반적인 U-Boot 기능을 수행한다. 다음 단계 이미지를 포함하는 부트 스크립트의 유효성이 검증되면, 제어권이 Linux 이미지로 전달되어 메모리에 적재된 후 실행된다. 이때 Linux 프롬프트에서 실행될 응용 프로그램 또한 서명하여 부팅 프로세스의 무결성을 보장할 수 있다.

3. TPM 기반 부팅 절차와 T2080 부팅 절차 비교분석

TPM과 T2080 프로세서는 공통적으로 부팅 프로세스의 무결성을 검증한다. TPM은 PCR에 각 부팅 프로세스의 무결성을 측정한 해시값을 저장하고, 부팅시 이를 비교하여 무결성을 검증한다. PCR 값은 기존의 해시값으로부터 확장하여 신뢰 체인을 형성하기 때문에 하드웨어의 변화를 모두 감지할 수 있으며, 실행될 운영체제의 무결성을 보장한다. T2080 프로세서는 시스템 코드의 해시값을 RSA 비대칭키를 사용해 디지털 서명을 생성하고 부팅 시 이를 비교함으로써 부팅 프로세스의 무결성을 검증한다. 또한 ITS(Intent to Secure) bit가 설정되면 공격자가 변조된 이미지로 부팅을 유도하더라도 부팅 프로세스를 중단할 수 있다.

그러나 리눅스 환경에서의 TPM은 위/변조되지 않은 운영체제가 부팅됐음에도 불구하고 런타임 공격에 대해 우회가 가능하다. TPM 자체는 CPU, 메모리와 완전히 격리되어 실행되므로 공격하기 어렵지만, PCR확장이나 해시값의 기록은 Trusted GRUB 등의 소프트웨어에서 명시적인 요구를 하는 경우에만 이루어지므로, Trusted GRUB을 공격함으로써 쉽게 이루어질 수 있다.[1]

반면 T2080 프로세서는 실행 가능 코드와 비실행 데이터 코드 사이의 메모리 파티셔닝 기능을 사용함으로써 런타임 공격으로부터 시스템을 보호할 수 있다. 또한 RTIC(Run Time Integrity Checker)를 사용하여 중요한 메모리 영역의 해시를 정기적으로 확인하고, 변조된 코드가 감지될 경우 시스템을 재설정함으로써 부팅 이후에도 시스템 코드의 무결성을 보장할 수 있다.

부팅 프로세스의 무결성을 보장하기 위해 암호화에 사용되는 키는 안전하게 저장되어야 한다. TPM은 외부에 저장된 다른 키를 보호하는데 사용되는 SRK(Storage Root Key)와 TPM을 식별할 수 있는 EK(Endorsement Key)를 가지고 있다. 이 키들은 TPM에서 제거할 수 없고 외부로 노출되지 않는 하드웨어적 특징 때문에 해당 TPM에서만 암호화된 데이터를 복호화할 수 있다. T2080 프로세서의 경우에는 OTPMK(One Time Programmable Master Key)와 KEK(Key Encryption Key)를 사용해 키를 암호화하며, 외부에 노출되지 않고 SEC(Security Engine)에서만 복호화를 진행하기 때문에 기밀 정보를 안전하게 보호할 수 있다.

4. 결 론

본 논문에서는 부팅 프로세스의 무결성을 보장하기 위한 신뢰성 컴퓨팅 기반의 시큐어 부팅 기술과 군사 무기체계 분야에서 활용되고 있는 화이트리스트 기반의 시큐어 부팅 기술을 분석하고 보안 관점에서 이를 비교하였다. TPM은 신뢰 체인을 구성함으로써 하드웨어의 변화를 감지하고 부팅 프로세스의 무결성을 검증할 수 있었다. T2080 프로세서는 신뢰할 수 있는 시스템 이미지를 사용하고 RSA 개인키가 안전하게 저장되면, 부팅 프로세스의 무결성 뿐만 아니라 운영체제가 부팅된 이후에도 시스템의 무결성 검증이 가능했다.

본 연구를 통해 신뢰성 컴퓨팅 환경은 부팅 프로세스의 무결성을 검증함으로써 운영체제가 위/변조 되지 않았음을 보장하고, 부팅 이후에도 시스템 이미지를 변조하려는 행위를 탐지하여 이를 예방할 수 있어야 함을 알 수 있었다. 또한 암호화 및 복호화에 사용되는 키는 외부로 유출되지 않고 시스템 내에서 안전하게 보호되어 인증되지 않은 사용자로부터 복호화를 방지할 수 있어야 함을 확인하였다. 군사용 드론의 컴퓨팅 환경은 물리적 보안 뿐 아니라 시스템 소프트웨어에 대한 보안도 중요하기 때문에 드론 시스템의 무결성 검증 기법이 필요하다. 따라서 무기 체계 드론의 수요가 급증하는 가운데 신뢰성 컴퓨팅 기반 시큐어 부팅 기술은 군사용 드론 시스템의 안전성을 높일 것으로 예상된다.

참 고 문 헌

[1] 이윤재, 유시환, “보안부팅+측정부팅 : 리눅스 부팅 과정의 무결성 보장”, 정보과학회 컴퓨팅의 실제 논문지, 제23권, 제8호, pp.504-509, 2017.

[2] Michael Slonosky, “Trusted boot in COTS computing”, Military Embedded Systems, 2015, http://mil-embedded.com/articles/trusted-boot-cots-computing/

[3] 박정숙, 한진희, 전성익, 조태남, “Trusted Computing 기술 및 TCG 표준화 동향”, 전자통신동향분석, 제2권, 제4호, pp.48-60, 2008.

[4] Raja Naeem Akram, Konstantinos Markantonakis and Keith Mayes, “An introduction to the trusted platform module and mobile trusted module”, Secure Smart Embedded Devices, Platforms and Applications, pp.71-93, 2014.

[5] TCG Specification, “Architecture Overview, Specifications Revision 1.2”, 2004.

[6] NXP Semiconductors, “QorlQ SDK v2.0-1703 Documentation”, 2017.

[7] Mike Slonosky, “Data Protection with the QORIQTM Platform T2080 Trust Architecture”, Curtiss-Wright, 2017.