Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.6, Dec. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.6.989

공급망 위협에 대응하기 위한 암호모듈의 안전한 부팅 보안 요구사항 제안

박 종 욱,†‡ 이 상 한, 구 본 석, 백 선 엽, 한 상 윤
ETRI 부설연구소 (연구원)

Secure Boot Security Requirements for Cryptographic Modules against Supply Chain Threats

Jong Wook Park,†‡ Sanghan Lee, Bonseok Koo, Seon Yeob Baek, Sang Yun Han
Affiliated Institute of ETRI (Researcher)

요 약

공급망 위협에 대응하기 위해 Secure Boot 등의 소프트웨어 위변조 방지 기술 및 SBOM(Software Bill of Materials) 등의 관리체계 개발 연구가 활발하게 이루어지고 있다. 특히 TCG(Trusted Computing Group)에서는 신뢰할 수 있고 안전한 컴퓨팅 부팅 환경을 제공할 수 있는 TPM(Trusted Platform Module) 표준을 제시하고 있다. 본 논문에서는 암호모듈이 공급망 위협에도 안전하고, 신뢰할 수 있는 기능을 제공할 수 있도록 암호모듈을 위한 안전한 부팅 기술 도입 필요성을 설명한다. 또한, ISO/IEC 19790 표준으로 검증된 암호모듈의 취약점을 분석하고, 취약점에 대응할 수 있도록 암호모듈의 안전한 부팅을 위한 보안 요구사항을 제안한다.

ABSTRACT

In order to respond to supply chain threats, active research and development efforts are underway for software tamper prevention technologies such as Secure Boot and management systems like Software Bill of Materials(SBOM). Particularly, the Trusted Computing Group (TCG) is introducing standards for Trusted Platform Module(TPM) to provide a secure and trustworthy computing boot environment. This paper emphasizes the need for introducing secure booting technology for cryptographic modules to ensure that they remain safe and provide reliable functionality even in the face of supply chain threats. Furthermore, it analyzes vulnerabilities in cryptographic modules verified by the ISO/IEC 19790 standard and proposes security requirements for secure booting of cryptographic modules to address these vulnerabilities.

Keywords: Supply Chain Threats, Root of Trust, Secure Boot, Trust Chain, ISO/IEC 19790

I. 서 론

정보화시대에 따른 IT 기술의 발달은 우리의 일상생활뿐만 아니라 산업 생태계에도 변화를 초래하여, 대부분의 제조업체는 제품의 설계로부터 생산 및 판매, 유지에 이르는 전 과정에서 다양한 하드웨어와 소프트웨어를 활용하고 있다. 공급망(Supply-Chain)이란 판매 제품의 생산, 유통, 유지에 요구되는 모든 부품과 서비스를 공급하는 개별 기업들의 집합을 의미한다. 이때 사용되는 하드웨어 및 소프트웨어는 제조·유통의 과정을 거쳐 기업에 공급되는데, 이러한 공급 과정에서 Fig. 1과 같이 데이터 위변조 및 각종 보안 위협에 노출될 수 있어 공급망 보안의 필요성이 지속적으로 제기되고 있다. 특히 하드웨어를 통

Received(10. 18. 2023), Modified(11. 08. 2023), Accepted(11. 22. 2023)
† 주저자, khspjw@nsr.re.kr
‡ 교신저자, khspjw@nsr.re.kr(Corresponding author)

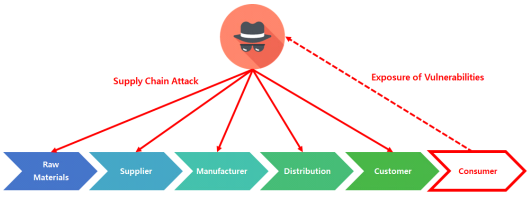

Fig. 1. Risk of Supply Chain

한 백도어 형태의 공격은 분석과 탐지가 매우 어려울 뿐만 아니라, 점차 확대되는 추세로 실제 이와 관련된 다양한 보안 사고들이 보고되고 있다[1].

이러한 공급망 보안 위협에 대응하도록 할 수 있는 대표적인 기술로 안전한 부팅(Secure Boot) 기술 등의 소프트웨어 위변조 방지 기술과 소프트웨어 공급망의 신뢰성과 투명성을 높일 수 있는 소프트웨어자료명세서(SBOM) 등의 취약점 관리 기술이 등장했다[2]. 또한 2023년 9월부터 소프트웨어가 안전하게 개발되었음을 미국 연방정부가 보증하는 자체증명서(Self-attestation) 제도를 시행하고 있다[3].

이중 안전한 부팅 기술은 부팅되는 소프트웨어의 위·변조를 탐지하고 변조된 소프트웨어의 부팅과 실행을 차단하는 기술로서 소프트웨어의 공급 과정에서 있을 수 있는 모든 종류의 악의적 조작과 악성코드를 방지할 수 있는 기술이다. Fig. 2는 시스코에서 제시하고 있는 신뢰할 수 있는 안전한 부팅 개념도이다[4]. 안전한 부팅의 신뢰 기반인 RoT(Root of Trust)는 하드웨어 Anchor가 담당한다. 하드웨어 Anchor에서 시작해 마이크로로더, 부트로더, 운영체제들은 각각 다음 단계의 소프트웨어를 검증하고, 해당 소프트웨어의 출처가 확인된 이후에 차례로 실행시킨다. 운영체제는 Trust Anchor 모듈에 대해 하드웨어 인증을 수행한 뒤 정상적인 모듈로 확인되면, 해당 모듈과 연동되는 중요 서비스를 동작시킨다. 이처럼 안전한 부팅 기술은 IT 시스템 내부의 전 영역에 걸쳐 존재한다.

안전한 부팅 기술은 크게 RoT 기술, 안전한 부트로더 기술, 운영체제에서 안전한 부팅 기술로 분류된다. 안전한 부팅의 RoT를 지원하는 상용 보안칩으로 Google의 Titan, Microsoft의 Cerberus, Apple의 T2, 삼성의 S3FV9RR, 많은 벤더에서 생산하는 TPM(Trusted Platform Module) 등이 있으며, 안전한 부팅 부트로더 기술은 MS의 UEFI-Secure-Boot와 TCG 그룹의 Trusted-GRUB2

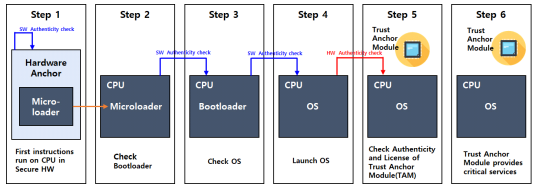

Fig. 2. Cisco's Trustworthy Secure Boot

등이 있다. 또한, MS Windows, MAC OS, SELinux 등의 운영체제들은 각자 고유의 메커니즘을 통해 안전한 부팅을 지원하고 있다[5-8].

암호모듈도 다른 IT 제품처럼 공급망 위협에 노출되어 있다. 암호모듈은 평가 기준인 ISO 19790에 따라 검증되지만, 외부 공격으로 암호모듈에 구현된 소프트웨어 또는 펌웨어가 변경될 수 있고, 변경된 소프트웨어에 또는 펌웨어에 대한 인증이 정상적으로 이뤄지지 않으면 언제든지 공급망 위협에 노출될 수 있다는 취약점이 존재한다. 따라서 검증된 암호모듈이 공급망 보안 위협으로부터 안전할 수 있도록 대책을 수립해야 한다. 운영체제에서 동작하는 소프트웨어 암호모듈은 해당 소프트웨어에 대한 해시 정보를 홈페이지에서 제공하기 때문에 암호모듈 무결성을 확인할 수 있다. 반면에, 펌웨어 암호모듈과 하이브리드 암호모듈의 경우에는 안전한 부팅 기술을 필수적으로 적용해야 공급망 보안 위협에 안전할 수 있다. 하지만, RoT 제품을 적용한 암호모듈의 안전한 부팅에 대한 보안 요구사항이 현재까지는 존재하지 않아 제조사별로 파편화되어 구현되었고, 이에 따라 공통적으로 적용할 수 있는 보안 요구사항 도출이 필요하다.

본 논문에서는 암호모듈 보안 요구사항에 대한 ISO/IEC 19790 표준에서 공급망 보안 위협에 대한 취약점을 분석하고, 안전한 부팅 기술 개발 동향을 살펴본다. 이후, 공급망 보안 위협에 대응하기 위해 암호모듈에 안전한 부팅 기술을 적용하는 방안을 제안하고, 안전한 부팅 기술을 암호모듈에 적용하기 위해 암호모듈 부팅 단계별 보안 위협, 보호 대상 식별, 대응 방안 및 보안 요구사항을 제시한다.

II. ISO/IEC 19790 표준 기반 암호모듈의 공급망 보안 위협

2.1 ISO/IEC 19790 동향

암호모듈 보안 및 시험 요구사항에 대한 최신 표

준은 ISO/IEC 19790:2012, ISO/IEC 24759:2017에 기술되어 있다[9,10]. 미국 NIST에서는 암호모듈 시험규격인 FIPS140-2를 ISO 표준과 독립적으로 적용했다. 하지만, 2019년 5월에 ISO 19790/24759를 수용하여 FIPS140-3으로 개정하고, 2020년 이후부터 해당 규격을 적용한 시험을 진행하고 있다. 한편, 국내에서는 ISO 규격을 바탕으로 작성된 KS X ISO/IEC 19790:2015, KS X ISO/IEC 24759를 시험에 적용하고 있다.

2019년부터 시작한 ISO/IEC 19790/24759 표준 개정 작업은 2024년 발간을 목표로 추진되고 있으며, 본 논문과 관련된 ISO/IEC 19790의 경우 공급망 위협에 대응할 수 있도록 "증명(Attestation)" 추가를 포함하여 237개 항목을 새롭게 혹은 변경할 예정이다[11].

본 절에서는 소프트웨어 또는 펌웨어의 변조 위협에 대응하기 위한 ISO/IEC 19790에 수록된 '7.7 소프트웨어·펌웨어 보안' 항목과 '7.4.3.4 소프트웨어·펌웨어 로드' 항목의 보안 요구사항들이 공급망 보안 위협에 효과적으로 대응할 수 있는지 분석한다.

2.2 ISO/IEC 19790의 소프트웨어·펌웨어 보안 항목 취약점

ISO/IEC 19790의 '7.7 소프트웨어·펌웨어 보안'은 소프트웨어 또는 펌웨어의 주입이 어려운 경우라고 가정한다. 보안등급이 가장 낮은 1등급은 무결성 검증, 2등급은 검증 대상 전자서명 또는 키 메시지 인증코드 검증, 그리고, 3등급 이상은 전자 서명 검증만을 적용하여 소프트웨어 또는 펌웨어의 안전성을 확인하도록 Table 1과 같이 요구하고 있다.

그러나, 위의 요구사항만으로 소프트웨어·펌웨어를 신뢰할 수 없다. 예를 들어 Fig. 3과 같이 1등급 암호모듈의 정상적인 펌웨어는 벤더가 제공하는 부트로더와 무결성 점검 펌웨어를 이용하여 신뢰성을 확

Table 1. Security Requirement of Not Loadable S/W,F/W in ISO 19790

Level	Security Requirement
1	Approved integrity technique
2	Approved digital signature or keyed message authentication code
3/4	Approved digital signature

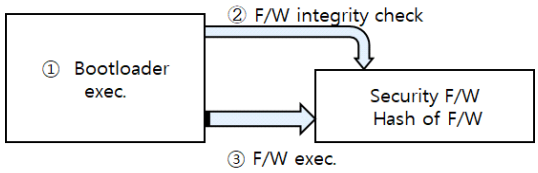

Fig. 3. F/W Security Requirements of ISO 19790 7.7

인한다.

이 경우 펌웨어의 안전성은 암호모듈 벤더를 신뢰하고, 검증된 보안 펌웨어를 암호모듈에 포팅했다는 가정이 필요하다. 하지만, 펌웨어의 해시 정보를 활용한 무결성 검증만 통과하면 무조건 보안 서비스를 실행한다는 취약점이 존재한다. Fig. 4와 같이 생산 단계에서 암호모듈의 부트로더를 수정하거나, 암호모듈의 펌웨어, 해시 정보 등을 수정하면 훼손된 보안 소프트웨어 또는 펌웨어가 정상적인 것처럼 실행될 수 있고, 운영자가 이를 확인하는 방법이 없다.

2등급 이상의 암호모듈도 앞에서 언급한 방법과 동일하게 부트로더를 수정하거나, 펌웨어, 인증키 등을 수정하면 훼손된 보안 소프트웨어 또는 펌웨어를 실행시킬 수 있다.

따라서, 소프트웨어 또는 펌웨어의 주입이 어려운 경우라고 가정하더라도 검증된 모듈의 소프트웨어 또는 펌웨어를 변경하여 임의의 소프트웨어 또는 펌웨어 실행을 근본적으로 방지할 수 있는 대책이 필요하다.

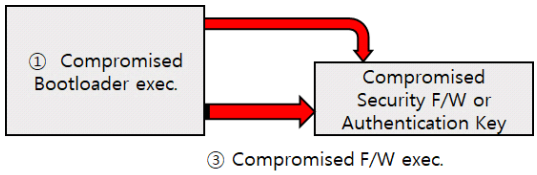

Fig. 4. Risk of Compromised Crypto Module I

2.3 ISO/IEC 19790의 소프트웨어·펌웨어 로드 항목 취약점

ISO/IEC 19790의 '7.4.3.4 소프트웨어·펌웨어 로드' 항목은 Table 2와 같이 소프트웨어 또는 펌웨어의 주입이 가능한 경우 보안등급과 관계없이 검증 대상에 대해 인증 메커니즘을 적용하고, 사용될 인증키는 소프트웨어 또는 펌웨어가 로드되기 이전에 독립적으로 암호모듈에 로드되어야 한다고 요구하고 있다[9].

현재까지 ISO 19790에는 승인된 인증 메커니즘이 제시되지 않았고, 국내에서도 별도로 제시하지 않

Table 2. Security Requirement of Loadable S/W,F/W in ISO 19790

Level	Security Requirement
1	- Approved authentication technique - Authentication key be loaded independently in the module prior to the software or firmware loading
2	
3	

고 있다. 미국은 허용된(allowed) 인증 메커니즘을 FIPS 140-3에서 Table 3과 같이 제시하고 있다[12].

소프트웨어 또는 펌웨어의 주입이 가능한 경우 암호모듈에 인증 기능을 적용하더라도 참조될 인증 키를 훼손하고, 암호 소프트웨어·펌웨어를 훼손하게 되면 실행되는 소프트웨어·펌웨어를 신뢰할 수 없게 된다. 예를 들어 Fig. 5와 같이 저장된 인증 키를 변경할 수 있거나 보안 펌웨어를 변경할 수 있는 경우 또는 부트로더를 변경할 수 있는 경우 보안 펌웨어 검증을 회피하거나, 훼손된 인증키로 검증을 통과하여 훼손된 소프트웨어·펌웨어를 실행할 수 있다.

지금까지 살펴본 바와 같이 ISO 19790의 보안 요구사항을 충족하는 것만으로는 암호모듈의 보안 소프트웨어·펌웨어가 공급망 보안에 안전하다고 할 수 없다. 따라서 암호모듈의 암호 소프트웨어·펌웨어를 신뢰하고, 공급망 보안의 위협에 대처할 수 있도록 추가적인 보안 요구사항 적용이 필요하다.

Table 3. Allowed Authentication Mechanism in FIPS140-3

Level	Authentication
1	▪ None required
2	▪ Memorized Secret or Level 3 Authentication
3	▪ Memorized Secret ▪ Look-Up Secrets ▪ Out-of_band ▪ Single-Factor OTP Device ▪ Multi-Factor OTP Device ▪ Single-Factor Crypto S/W ▪ Single-Factor Crypto Device ▪ Multi-Factor Crypto S/W ▪ Multi-Factor Crypto Device
4	▪ Multi-Factor Crypto S/W ▪ Multi-Factor Crypto Device

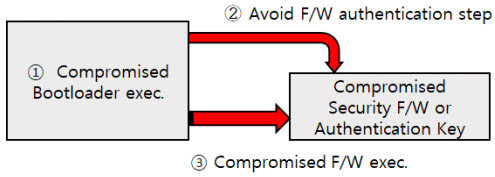

Fig. 5. Risk of Compromised Crypto Module II

III. 안전한 부팅 관련 연구 동향

3.1 안전한 부팅 개념 및 개발 현황

안전한 부팅은 Fig. 6과 같이 RoT에서 출발하여 연쇄적으로 연결된 계층의 바이너리 코드의 무결성이 훼손되지 않았음을 보장하는 방법이다. RoT는 시스템의 보안성을 보장하기 위해 부팅 과정에서 가장 먼저 실행되며, 이를 통해 시스템의 다음 단계가 신뢰할 수 있는 소프트웨어로만 구성되었음을 보장할 수 있고, 어떤 방법으로도 변경 불가능한 소스 코드로부터 시작하도록 하는 기술로 정의할 수 있다.

안전한 부팅 구현을 위해 신뢰성이 검증된 최하위 단계의 BootROM 코드를 비롯하여 해시 알고리즘, 공개키 인증서와 같은 보안 알고리즘과 시스템에 탑재한 별도의 보안 회로와 같은 보안 설계를 통해 RoT를 일반적으로 제공한다. 하지만, 빠른 부팅을 위해 일반적으로 알고리즘 보안 강도가 낮게 설정되어 있다.

안전한 부팅은 부팅 과정에서 상위 단계로 전환이 발생하는 경우 RoT를 기반으로 상위 단계의 무결성을 하위 단계에서 검증한다. 만일 부팅 단계에서 무결성에 문제가 발생하는 경우 심각한 오류를 알려주거나, 오류 메시지를 출력하고 부팅을 진행하거나, 또는 시스템을 보호할 수 있도록 추가적인 조치를 수행한다. 안전한 부팅과 관련된 상용제품은 Table 4와 같이 시스템의 사용 환경과 시스템의 하드웨어 사양, 사용 목적에 따라 다양한 제품이 생산되고 있다.

안전한 부팅 기술은 프로세서의 하드웨어에 많은 영향을 받는 계층으로 Intel, Apple, ARM, Samsung 등과 같은 프로세서 제조사마다 각자의

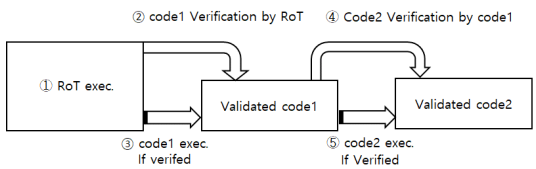

Fig. 6. Secure Boot Conceptual Diagram

Table 4. Commercial Products and Technology for Secure Boot

Category	Examples
RoT Chip Products	Intel Boot Guard, ARM TrustZone, Samsung KNOX, Google Titan, Apple T2 Chip, Microsoft Cerberus chip, etc
Secure Bootloader Technology	Intel BIOS Guard, GNU Trusted GRUB, UEFI forum UEF-Secure-Boot, Linux forum Shim, NIST Platform Firmware Resiliency Guideline, Microsoft Cerberus project F/W

독자적 기술을 사용한다. 프로세서 시장의 대부분을 차지하고 있는 Intel의 경우, 보안상의 이유로 관련 기술을 완전히 공개하지 않고 있다. 보드 개발자들이 특정 프로세서를 선택하는 순간 해당 프로세서가 제공하는 안전한 부팅 기술을 사용해야 하며, 공개되지 않는 기술 영역의 경우 해당 기술의 안전성에 대한 확인 과정 없이 사용해야 한다. 따라서 안전성이 확인된 안전한 부팅 기술을 사용하기 위해서 제조사 기술에 종속되지 않고 공통적으로 적용할 수 있는 보안 요구사항을 도출할 필요가 있다.

PC에 적용되는 안전한 부팅 기술은 Microsoft가 주도하는 UEFI(Unified Extensible Firmware Interface)로 플랫폼 펌웨어와 운영체제 사이를 정합하는 부트로더 펌웨어의 표준이다. UEFI 2.3.1 버전부터 안전한 부팅 기술을 포함하고 있고, 부트로더 펌웨어 인증에 필요한 서명값과 공개키의 발급을 Microsoft가 담당하게 하고 있다. Linux 진영에서는 UEFI 펌웨어를 사용하는 PC(노트북)에서 Linux를 부팅시키기 위하여, Linux 부트로더(u-Boot, GRUB 등)와 UEFI 사이에 Microsoft가 서명한 부트로더 'shim'을 두어 사용자들이 Linux 운영체제를 사용할 수 있도록 하고 있으며, Apple의 MAC OS의 경우 UEFI를 사용하지 않고 T2 칩을 이용한 독자적인 안전한 부팅 기술을 적용하고 있다.

3.2 기존 안전한 부팅 기술을 암호모듈에 적용하기 위한 한계점

상용화된 대부분의 안전한 부팅은 자사 제품군에 대한 최적화된 보안을 위해 개발되었다. UEFI 부팅의 경우 Microsoft의 인증을 통한 UEFI와의 기술 협약 없이는 UEFI 환경에서의 안전한 부팅을 개발할 수 없는 한계가 있으며, 임베디드 환경에서의 안전한 부팅 개발은 제조사별로 다른 H/W 환경으로 인해 서로 다른 안전한 부팅 모델과 규격, 제조사에 대한 의존성이 생기게 된다. 임베디드 환경에서 규격화되지 않은 안전한 부팅 방식은 소규모 임베디드 환경에서 개발이 중단, 지연되는 원인이 될 수 있으며, 보안업체와의 기술 협약의 경우 기술에 대한 비용이 많아질 수 있다.

또한 상용제품의 경우 안전한 부팅 기술은 응용소프트웨어나 운영체제에 대한 악의적인 위변조를 탐지하는 기술에 국한되어 있으며, 무결성 검증에만 집중되어 있다.

프로세서 제조사, 운영체제 개발사 별로 통일되지 않은 안전한 부팅 기술들이 사용되고 있으며, 따라서 임베디드 시스템 개발자들은 개발 보드의 프로세서와 적용 운영체제에 따라 각기 다른 안전한 부팅 기술을 적용해야 하는 불편함을 감수해야만 한다.

2017년 이후 안전한 부팅 기술에 대한 공통의 표준기술 개발을 위한 노력으로 Google의 Titan, NIST의 Platform Firmware Resilience Guideline(SP 800-193) 그리고 Microsoft의 Cerberus project, GlobalPlatform의 Root of Trust 표준화가 추진되고 있다.

암호모듈에 상용제품을 적용하여 안전한 부팅을 구현하기 위해서는 운영체제, 프로세서와 무관하게 공통으로 적용할 수 있는 보안 요구사항 개발이 필요하다.

3.3 안전한 부팅을 위한 요구사항 개발 사례

GlobalPlatform은 모바일 기기를 해커, 악성 응용프로그램 등으로부터 안전하게 보호할 수 있도록 민감한 자산과 코드에 대해 격리된 실행환경을 제공할 수 있는 연구를 수행하였다. 또한 2018년에 플랫폼의 안전한 서비스를 제공하기 위해 많은 업체가 독립적으로 제시하고 있는 안전한 부팅 기술의 핵심 요소인 RoT 요구사항 표준을 제시하였다[13].

본 논문에서는 GlobalPlatform에서 제시한 RoT 요구사항 중에서 암호모듈과 같이 규모가 작은 플랫폼에 적용이 가능한 Table 5의 RoT가 1개로 구성된 non-bootstrapped RoT 요구사항을 암호모듈의 안전한 부팅을 위한 보안 요구사항 도출에 적용한다.

Table 5. Requirements of Non-Bootstapped RoT

Category	Requirements
1. Computing Engine, Code, and Data	Root of Trust SHALL consist of a computing engine and executable code.
2. Security Services	Root of Trust SHALL provide one or more security services (authentication, authorization, confidentiality, identification, integrity, measurement, reporting, update, and verification).
3. Certification	Vendor/Manufacturer SHALL design a Root of Trust for a certification process for a platform or for a device.
4. Unique Identifiable Ownership	Root of Trust SHALL have a single identifiable owning entity.
5. Mutability	Code and/or data of a Root of Trust SHALL be immutable or its mutability SHALL be controlled only by the unique identifiable owner.
6. Ownership Transfer	If a Root of Trust implements an ownership transfer mechanism designed by the initial owner/provider of the RoT, then the current owner of the Root of Trust SHALL provide a mechanism to authorize the transfer of ownership to the new owner.
7. One RoT per Platform	A Platform SHALL contain one and only one Root of Trust.
8. Temporal	Root of Trust SHALL include the code which executes first upon the initialization of the computing engine during cold boot in that platform.
9. Manufacturer Identity	Root of Trust SHALL have an identifiable manufacturer
10. Provenance	Platform manufacturer SHALL create and provision the Root of Trust during the manufacturing process.

암호모듈의 안전한 부팅을 위한 보안 요구사항을 도출하기 위해 암호모듈의 부팅 모델 제시, 보호대상 식별 및 위협분석, 대응방안 제시, 보안 요구사항 도출 순서로 다음 절에서 제안한다.

IV. 공급망 위협에 대응하기 위한 암호모듈의 안전한 부팅을 위한 보안요구사항 제안

본 절에서는 암호모듈을 공급망 위협으로부터 안전하게 보호하기 위해, 일반화된 암호모듈 부팅 모델을 제시하고, 암호모듈 구성요소 중 보호해야 할 대상 식별과 보호 대상별 보안 위협을 기술한다. 또한 상용제품을 이용한 암호모듈의 안전한 부팅 모델과 보안 요구사항을 제시한다.

본 논문에서 제안하는 안전한 부팅 모델은 CPU를 내장하고 있는 암호모듈을 적용 대상으로 한다. 이러한 암호모듈은 CPU가 구동하는 펌웨어와 소프트웨어 또는 하드웨어 암호가속기를 이용하여 보안서비스를 제공한다.

4.1 암호모듈 부팅 모델, 보호대상 및 보안위협

Sara Zimmo 등은 임베디드 디바이스의 부팅 방법을 사전부트(Preboot), 부트로더(bootloader), 운용체제 및 응용 로더의 3단계 모델을 적용하고 있다[14,15]. 암호모듈에 대해서도 Fig. 7과 같이 3단계 부팅 모델로 가정하면, 수정할 수 없는 제조사 영역인 Boot ROM에서 시작하여 벤더가 제공하는 1단계 부트, 보안서비스 소프트웨어·펌웨어를 로드하는 2단계 부트, 응용 프로그램 및 OS를 로더하는 3단계 부트로 모델링할 수 있다.

Fig. 7의 암호모듈 부팅 모델에서 부팅 단계별 공급망 위협의 대상이 되는 보호대상과 위협을 세분화시키면 Table 6과 같다.

1단계 부트에서는 벤더 부트 펌웨어와 소프트웨어·펌웨어 인증 키, 설정 데이터를 보호대상으로 분류하고, 2단계 부트에서는 보안서비스를 제공하는 소프트웨어·펌웨어를 보호대상으로 분류하며, 3단계 부트에서는 응용 프로그램 및 운영체제를 보호대상으로 분류한다. 그리고 모든 단계에서는 신뢰할 수 없는 객체에 의한 위·변조 위협에 대한 보호대책이 필요하다. 1단계 부트의 벤더 부트 펌웨어와 설정 데이터의 경우, 지금까지는 제조사 영역이라는 이유

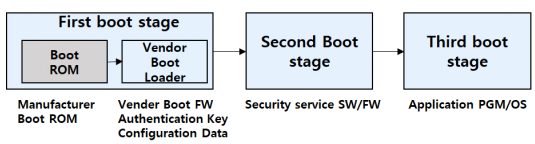

Fig. 7. Generalized Boot model of Crypto Module

Table 6. Protected Objects and risks of Crypto Module

Protected Objects		Boot Stage	Risks
Vendor Boot F/W		1	Unauthorized modification, substitution
Authentication Key		1	
Configuration data		1	
Security S/W or F/W	Asymmetric Cryto Alg.	2	
	Symmetric Crypto Alg.		
	HASH/MAC		
	RNG		
	Key Generation		
	Digital Signature		
	Key Agreement		
	Self Diagnonis		
	Authentication		
	Logging		
Application Program		2	
OS		2	

로 검증대상에서 제외되었지만, 안전한 부팅을 위해 추가적인 검증이 필요하다.

암호모듈 운용 중에 주입되거나 생성되는 보안 매개변수(security parameters)의 경우에는 안전한 부팅과 무관하므로 보호대상에서 제외하고, 보안 서비스 소프트웨어 또는 펌웨어에서 보호되도록 해야 한다.

4.2 상용제품을 이용한 안전한 부팅 구현 분류

RoT 상용제품을 활용한 암호모듈의 안전한 부팅은 다음과 같이 2가지로 크게 분류할 수 있다. 첫째, Fig. 8-(A)와 같이 CPU에서 제공하는 RoT 기능을 활용하여 안전한 부팅을 구현할 수 있다. 둘째, Fig. 8-(B)와 같이 별도의 RoT 하드웨어 칩을 이용하여 안전한 부팅을 구현할 수 있다. 별도의 RoT 칩을 이용할 경우, RoT는 외부 플래시 메모리의 부트로더를 인증하기 전까지는 CPU 동작을 보류하고, 인증을 완료한 후에 CPU가 동작할 수 있도록 제어해야 한다.

구현 방법에 상관없이 RoT는 데이터의 무결성을 보장할 수 있도록 인증 동작에 필요한 키를 내부의

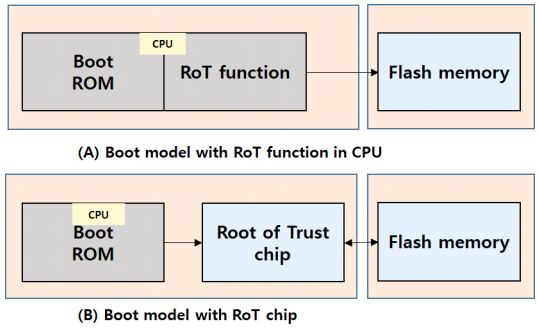

Fig. 8. Secure Boot Methods Using Commercial Products

OTP(One Time Programmable) 메모리에 저장해야 한다. OTP 메모리는 저장 데이터의 변경·삭제가 불가능하여 데이터 무결성을 보장할 수 있는 특성을 갖는다. 따라서, RoT 기능이 내장되면 OTP 메모리 또는 이와 유사한 기술을 활용하여 인증 키를 저장하는 기능이 필수적이다[16].

4.3 RoT를 이용한 암호모듈의 안전한 부팅 모델

기존 임베디드 시스템 환경에서 RoT 기능을 지원하는 TPM 칩을 이용하여 소프트웨어의 변조를 감지하는 방식이 제시되었다[17-19]. 그러나 다양한 위협 시나리오에서 안전한 부팅 기술을 활용하여 어떤 대상을 보호하고, 어떤 방식으로 대응하며, 이에 대한 보안요구사항을 포함한 안전성 평가 기준에 관한 연구는 현재까지 구체적으로 추진되지 않았다. 따라서 암호모듈의 안전한 부팅을 위한 보안 요구사항을 도출하기 위해 Fig. 7의 암호모듈 부팅 모델을 참조하여 RoT 상용제품을 적용한 암호모듈의 안전한 부팅을 위해 Fig. 9와 같이 3단계로 인증을 수행하는 부팅 모델화하였다. Fig. 9의 모델은 암호모듈의 CPU에서 RoT 기능을 제공하는 경우와 별도의

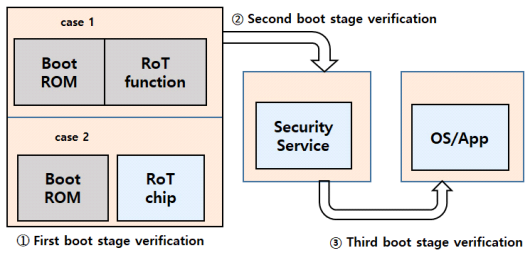

Fig. 9. Secure Boot Model for Cryptographic Modules

RoT 칩을 이용하는 경우에 모두 적용할 수 있고, 상용 암호모듈에 범용적으로 적용할 수 있다.

암호모듈의 안전한 부팅 절차는 RoT를 기반으로 하는 첫 번째 부팅 단계에서 부트롬과 설정 데이터 등의 무결성을 검증한 후 이상이 없으면 다음 단계의 무결성을 순차적으로 검증하는 신뢰체인방식을 적용한다. 만일 각 부팅 단계에서 무결성이 훼손된 계층을 발견하는 경우 부팅을 멈추고, 경고 메시지를 출력하여 위변조 공격을 원천적으로 차단할 수 있어야 한다. 다음 절에서는 Table 6의 암호모듈 보호대상을 안전하게 보호할 수 있도록 안전한 부팅을 위한 부팅 단계별 보안 요구사항을 제안한다.

4.4 RoT를 이용한 암호모듈의 안전한 부팅을 위한 보안 요구사항 제안

암호모듈에 안전한 부팅 기술을 적용하고, 제안하는 보안 요구사항을 만족하면 완전한 신뢰체인을 구성하여 암호모듈에 탑재된 소프트웨어 또는 펌웨어에 대한 위변조 공격을 원천적으로 차단할 수 있으며, 암호모듈을 공급망 보안 위협으로부터 안전하게 보호할 수 있다.

Table 6의 보호대상별 위협에 대응하기 위해 Fig. 9의 안전한 부팅 모델에서 부팅 단계별로 위협과 대응방안 그리고 그에 따른 요구사항을 다음과 같이 제안한다.

첫 번째 부팅 단계는 RoT가 부팅되는 단계로 Table 7과 같이 위협과 대응방법, 요구사항을 3가지 분류로 제안한다.

첫째, 신뢰의 근원이 되는 RoT 기능이 포함되어야 한다. RoT 기능에 대한 보안 요구사항은 Table 3과 같이 GlobalPlatform에서 제안한 요구사항 중 검증과 제작사와 관련된 Certification 항목과 Manufacturer Identity 항목을 제외한 8개 항목으로 제안한다.

둘째, 부트 펌웨어·설정 데이터 위·변조 위협에 대응하기 위해 부트 펌웨어·설정 데이터 위·변조로부터 보호해야 하며, 2개의 요구사항을 제안한다.

셋째, 소프트웨어·펌웨어 인증 키의 신뢰할 수 없는 객체에 의한 위·변조 위협에 대응하기 위해 소프트웨어·펌웨어 인증 키의 신뢰할 수 없는 객체에 의한 위·변조로부터 보호해야 하며, 4개의 요구사항을 제안한다. OTP에 저장해야 하며, 물리적 위협으로부터 안전해야 한다는 요구사항이 인증 키에 대한 요구사항에 추가되었다.

Table 7. Security Requirements of 1st Boot Stage

1st Boot Stage	
Threat	Threat of injecting malicious attack code of some sort prior to start of the chain of trust to gain low-level and nearly undetectable control over the system
Response	First boot stage SHALL have function of RoT
	〔Requirement 1〕 First boot stage SHALL consist of a computing engine and executable code.
	〔Requirement 2〕 First boot stage SHALL provide one or more security services(authentication, authorization,identification, integrity, verification)
	〔Requirement 3〕 First boot stage SHALL have a single identifiable owning entity.
	〔Requirement 4〕 Code and/or data of first boot stage SHALL be immutable or its mutability SHALL be controlled only by the unique identifiable owner.
	〔Requirement 5〕 If first boot stage implements an ownership transfer mechanism, first boot stage SHALL provide a mechanism to authorize the transfer of ownership to the second boot stage.
	〔Requirement 6〕 First boot stage SHALL contain one and only one Root of Trust.
	〔Requirement 7〕 First boot stage SHALL include the code which executes first upon the initialization of the computing engine during cold boot in that platform.
	〔Requirement 8〕 platform manufacturer SHALL create and provision the first boot stage during the manufacturing process.

1st Boot Stage	
Threat	Boot firmware/configuration data tampering threat
Response	Boot firmware and configuration data SHALL be protected from tampering and alteration.
	〔Requirement 9〕 First boot stage SHALL detect any tampering or alteration of the boot firmware and configuration data.
	〔Requirement 10〕 When the first boot stage confirms the tampering or alteration of the boot firmware and configuration data, first boot stage SHALL prevent the use of the compromised boot firmware and configuration data.
Threat	Threat of tampering and alteration by untrusted entities of software/ firmware authentication keys
Response	Software/firmware authentication keys must be protected to prevent external leakage or tampering during usage
	〔Requirement 11〕 Software/firmware authentication keys must be stored in One Time Programmable (OTP) memory space.
	〔Requirement 12〕 First boot stage shall detect any tampering or alteration of the software/ firmware authentication keys.
	〔Requirement 13〕 When first boot stage confirms the tampering or alteration of the software/firmware authentication keys, it must prevent the use of the compromised software/ firmware authentication keys.
	〔Requirement 14〕 The software/firmware authentication keys must be secure against physical security threats.

첫 번째 단계의 부팅이 성공적으로 수행되면 보안 서비스 소프트웨어·펌웨어를 로딩하는 두 번째 부팅 단계를 수행한다. 두 번째 부팅 단계에서는 보안 서비스 소프트웨어·펌웨어를 위·변조로부터 보호할 수 있도록 Table 8과 같이 2개의 요구사항을 제안한다.

Table 8. Security Requirements of 2nd Boot Stage

2nd Boot Stage	
Threat	Software/firmware tampering threat for security services
Response	Security services software/ firmware must be protected from tampering and alteration.
	〔Requirement 15〕 Second boot stage must be able to detect any tampering or alteration of software/firmware for security services.
	〔Requirement 16〕 When the second boot stage detects tampering or modifications in the software/firmware, it must prevent the use of the tampered or modified software/firmware.

두 번째 단계의 부팅이 성공적으로 수행되면 응용프로그램·운영체제를 로딩하는 세 번째 부팅 단계를 수행한다. 세 번째 부팅 단계에서는 응용프로그램·운영체제 위·변조 위협에 대응하기 위해 프로그램·운영체제를 위·변조로부터 보호할 수 있도록 Table 9와 같이 2개의 요구사항을 제안한다.

Table 9. Security Requirements of 3rd Boot Stage

3rd Boot Stage	
Threat	Applications/OS tampering threat
Response	Applications/OS must be protected from tampering and alteration.
	〔Requirement 17〕 Third boot stage must be able to detect any tampering or alteration of applications/OS.
	〔Requirement 18〕 When the third boot stage detects tampering or modifications in the applications/OS, it must prevent the use of the tampered or modified applications/OS.

V. 결 론

본 논문에서는 암호모듈이 ISO/IEC 19790 표준에 따라 검증되더라도 내부 암호 소프트웨어 또는 펌웨어가 공급망 보안 위협에 쉽게 노출될 수 있음을 확인했고, 이에 대처할 수 있도록 암호모듈의 안전한 부팅 기술 도입 필요성을 살펴보았다. 하지만, 현재까지 암호모듈에 안전한 부팅 기술을 적용하기 위한 보안 요구사항이 존재하지 않고, RoT 제조사별로 기능과 요구사항이 다양하게 구현되어있어, 이를 해결할 수 있도록 RoT를 이용한 암호모듈의 안전한 부팅을 위한 보안 요구사항을 다음과 같이 도출하였다.

첫째, 안전한 부팅을 적용하지 않은 암호모듈의 부팅 단계별 보호 대상, 보안 위협 및 대응방안을 제안하였다. 둘째, 암호모듈에 탑재된 암호 소프트웨어 또는 펌웨어를 신뢰할 수 있고, 공급망 보안의 위협에 근본적으로 대처할 수 있도록 RoT를 이용한 암호모듈의 3단계 안전한 부팅 모델을 설정하였다. 셋째, 암호모듈의 안전한 부팅을 수행하기 위해 부팅 단계별로 위협과 대응방안 및 보안 요구사항을 제안하였다.

제안한 보안 요구사항은 ISO 19790 표준에 반영될 경우 암호모듈에 내장된 소프트웨어 또는 펌웨어를 공급망 보안 위협에 대응할 수 있으며, ISO 19790에 새롭게 추가될 증명(attestation) 항목의 구현 요구사항으로도 활용될 수 있다.

References

[1] Daewon Kim, Dongwook Kang, Yongje Choi, Sangsu Lee, Byeongcheol Choi, "Trends in Supply-Chain Security Technologies," Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157, Aug. 2020.

[2] Yunseong Choi, "Trends in Software Supply chain Security Polices in USA: : A focus on SBOM", KIISC, Vol.32, No.5, pp7-14, Oct. 2022.

[3] Cybersecurity and Infrastructure Security Agency(CISA), "Secure Software Development Attestation Form Instructions", https://www.cisa.gov/sites/default/files/2023-4/Secure-Software-self-attestation-form_508.pdf, Apr. 2023.

[4] Cisco, "Cisco Trustworthy Technologies Data Sheet," https://cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf, 2023.

[5] J. Frazelle, "Securing the Boot Process: The hardware root of trust," ACM Queue, vol. 17, no. 6, pp.5-21, Dec. 2019.

[6] OpenTitan, https://opentitan.org/, Oct. 2023

[7] Intel Information Technology Cybersecurity, "Intel® Hardware Shield-Below-the-OS Security," White Paper, May 2021.

[8] R. Wilkins, B. Richardson, "UEFI Secure Boot in Modern Computer Security Solutions", Sep. 2013.

[9] ISO/IEC 19790:2012, "Information technology -Security techniques-Security requirements for cryptographic modules," Aug. 2012.

[10] ISO/IEC 24759:2017, "Information technology -Security techniques-Test requirements for cryptographic modules," Mar. 2017.

[11] Graham Costa, "ISO 19790:2024 and 24759:2024 - How is progress and what has changed?", International Cryptographic Module Conference 2023, Sep. 2023

[12] K. Schaffer, "CMVP Approved Authentication Mechanisms," NIST SP 800-140E, Mar. 2020.

[13] GlobalPlatform Technology, "Root of Trust Definitions and Requirements Version 1.1.1," Jun. 2022.

[14] Rui Wang, Yonghang Yan, "A Survey of Secure Boot Schmes for Embedded Deivces", International Conference on Advanced Communications Technology (ICACT), pp. 224-227., Feb. 2022.

[15] Sara Zimmo, Ahmed Refaey, Abdallah Shami, "Trusted Boot for Embedded Systems Using Hypothesis Testing Benchmark", 2020 IEEE Conference on Electrical and Computer Engineering

(CCECE), Sep. 2020

〔16〕 Andres Meza, Francesco Restuccia, Jason Oberg, Dominic Rizzo, Ryan Kastner, "Security Verification of the Open Titan Hardware Root of Trust", IEEE Security & Privacy, Vol 21,pp. 27-36, May-June 2023.

〔17〕 Jin-Woo Kim, Sang-Gil Lee, Jae-Yong Ko, Cheol-Hoon Lee, "An Implementation of Secure boot Using TPM in Embedded System," Journal of The Korea Institute of Information Security & Cryptology, vol. 29, no. 5, Oct. 2019.

〔18〕 V. Mattila, P. Dwivedi, P. Gauri and D. Dadhich, "Hardware Root of Trust Based TPM: The Inherent of 5irechain Security," International Journal of Social Sciences and Management Review, vol. 5, no. 3, pp. 248-258, Jun. 2022.

〔19〕 Promila, Jyothi T., Shilpa Jain, "TPM Based Secure Boot in Embedded Systems," 2023 Third International Conference on Secure Computing and Communication(ICSCCC), pp. 786-790, May 2023.

〈저자소개〉

박 종 욱 (Jong Wook Park) 정회원
1986년 2월: 경북대학교 전자공학과 졸업
1988년 2월: 경북대학교 전자공학과 석사
2001년 8월: 경북대학교 전자공학과 박사
1988년 2월~2000년 1월: 국방과학연구소 연구원
2000년 2월~현재: ETRI 부설연구소 책임연구원
〈관심분야〉 암호검증, 블록체인, AI 보안

이 상 한 (Sanghan Lee) 정회원
1994년 2월: 경북대학교 전자공학과 졸업
1997년 2월: 경북대학교 전자공학과 석사
2016년 2월: 경북대학교 전자공학과 박사
1997년 2월~2000년 1월: 국방과학연구소 연구원
2000년 2월~현재: ETRI부설연구소 책임연구원
〈관심분야〉 VLSI 설계, 암호 SoC, RoT, 시큐어부팅

구 본 석 (Bonseok Koo) 정회원
1998년 2월: 경북대학교 전자공학과 졸업
2000년 2월: 포항공과대학교 전자공학과 석사
2009년 2월: 고려대학교 정보보호대학원 박사
2000년 10월~현재: ETRI부설연구소 책임연구원
〈관심분야〉 암호모듈 검증, 암호칩 설계, PQC암호 구현

백 선 엽 (Seon Yeob Baek) 종신회원
2003년 2월: KAIST 전기 및 전자공학과 졸업
2010년 1월: KAIST 전기 및 전자공학과 박사(석박통합)
2010년 2월~11월: KAIST 전기 및 전자공학과 포닥
2010년 12월~현재: ETRI 부설연구소 책임연구원
〈관심분야〉 AI보안, 인증, 네트워크 보안, 무선통신

한 상 윤 (Sang Yun Han) 정회원
2002년 2월: 홍익대학교 전자전기공학과 졸업
2004년 2월: 포항공과대학교 정보보안 석사
2004년 2월~현재: ETRI 부설연구소 실장
〈관심분야〉 암호검증, 정보보호, 암호