TPM 기반 안티탬퍼링 솔루션을 통한 무기체계 기술 보호

TPM-Based Anti-Tampering Solutions to Protect Weapon Systems Technologies

이재호 (J.H. Lee, bigleap@etri.re.kr) 국방사이버전기술연구센터 책임연구원/기술총괄
김도형 (D.H. Kim, kimdh@etri.re.kr) 국방사이버전기술연구센터 책임연구원
이형석 (H.S. Lee, hyslee@etri.re.kr) 국방사이버전기술연구센터 책임연구원
한진희 (J.H. Han, hanjh@etri.re.kr) 국방사이버전기술연구센터 책임연구원
김영세 (Y.S. Kim, vincent@etri.re.kr) 국방사이버전기술연구센터 책임연구원
류철 (C. Ryu, ryuch@etri.re.kr) 국방사이버전기술연구센터 선임연구원
최예슬 (Y.S. Choi, yeseul@etri.re.kr) 국방사이버전기술연구센터 연구원
이윤경 (Y.K. Lee, neohappy@etri.re.kr) 국방사이버전기술연구센터 책임연구원/센터장
김정녀 (J.N. Kim, jnkim@etri.re.kr) 사이버보안연구본부 책임연구원/본부장

ABSTRACT

Protecting weapon system technologies is essential for national security. Advancements in artificial intelligence and South Korea's growing role in the global defense market underscore the importance of anti-tampering technologies. TPM-based anti-tampering ensures the integrity and confidentiality of weapon systems. This paper analyzes the concept of anti-tampering and the current standards and technologies related to TCG's TPM/TSS. With mandatory integration requirements for exported weapon systems, TPM-based anti-tampering solutions provide cost-effective, high-level security while effectively safeguarding K-Defense technologies.

KEYWORDS TCG, TPM, TSS, 안티탬퍼링

Ⅰ. 서론

현대 국방 환경의 변화와 첨단 기술 도입으로 인해 국가 안보와 관련된 기술 보호의 중요성이 커지고 있다. 국방혁신 4.0[1]에 따르면 AI 등 첨단 기술을 국방 분야에 적용하여 군사 작전의 효율성을 강화하고자 한다. 한편, 첨단 기술 도입은 자율주행 무기체계의 분실 및 탈취 위험성과 수출 무기에 대한 불법적 기술 분석에 대응할 필요성을 높이고 있다.

본고에서 수출용 무기체계의 기술 보호 필요성과 안티탬퍼링 구현 방법 중 HW 기반 보안 솔루션과 밀접한 TCG[2]의 TPM[3]과 TSS[4] 표준 및 기술

* DOI: https://doi.org/10.22648/ETRI.2024.J.390506
* 이 논문은 2023년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임[KRIT-CT-22-051, 무기체계기술 보호기법 핵심기술 개발과제].

현황을 살펴본다. 수출용 무기체계에 대한 안티탬퍼링 기술 탑재 의무화로, TPM은 저비용으로 무기체계의 부팅 무결성, 플랫폼/응용 변조 방지, 암호화 키 및 인증서 저장, 중요 데이터 보호 등 높은 수준의 보안을 요구하는 국방 응용에 활용도가 높을 것으로 예상된다.

II. 안티탬퍼링

1. 무기체계 기술 보호의 필요성

가. 국내 무기체계 수출 현황

한국의 방산 수출은 K-2 전차, K-9 자주포, FA-50 경공격기 및 K-239 천무 다연장 로켓 시스템을 포함한 폴란드와의 계약으로 2022년 사상 최고치인 173억 달러(약 23조 원)를 기록했다[5].

K-방산은 첨단 기술과 가격 경쟁력으로 세계 무기 시장 10위권에 진입했으며, 2027년까지 글로벌 수출 점유율 5%를 넘어 세계 4대 방산 수출국으로 도약하려는 목표를 가진다. 더불어 수출 무기체계의 기술 보호가 점점 중요해지고 있다[6].

나. AI 탑재 무인 무기체계 증가

국방혁신 4.0은 AI와 첨단 기술을 활용해 현대 전장에서 효과적인 방위 능력을 구축하는 것을 목표로 하며, 유인 및 무인 시스템이 협력하는 AI 기반 유무인 복합전투 체계(MUM-T) 구축을 목표로 한다[7,8].

지상(자율 차량, 전투 로봇), 해양(무인 수상정 또는 잠수함, 해양 드론), 공중(자율 비행 드론, 무인 전투기) MUM-T 체계를 구성하는 AI 탑재 무기체계 개발 사례들은 다음과 같다.

- 드론 작전 사령부: 북한 무인 정찰기 침입에 대응할 수 있는 감시 및 전투 수행용 소형 드론
- 국방과학연구소(ADD): AI를 활용해 최적 경로를 판단하고 인명 피해를 줄이는 자율주행 무인 군사 차량
- LIG넥스원: 자율 운행을 통해 지뢰를 탐지하고 해군의 지뢰 제거 작전을 지원하는 AI 기반 해저 지뢰 탐지 시스템
- LIG넥스원: 적의 움직임을 AI로 분석하고 대응하는 AI 기반 전투 잠수함

이러한 AI 탑재 무기체계는 복잡한 알고리즘과 많은 양의 데이터 기반 의사결정으로 인해 예기치 못한 상황이나 시스템 오류 시 적진에서 분실 또는 탈취될 위험이 있다.

다. 기술 유출 사례

첨단 무기체계는 적의 위협을 실시간 분석하고 대응하지만, 적에게 노출되면 AI 알고리즘의 역설계와 조작으로 역공격 위협에 처할 수 있다. 다음은 미국의 기술 유출 사례다.

- ('07년) 중국의 F-35 전투기 설계도 탈취를 통한 청두 J-20 스텔스 전투기 개발 가속화[9]
- ('11년) 이란의 RQ-170 센티넬 드론 포획[10]
- ('11~'12년) 이란의 드론 해킹 및 제어 주장[11]
- ('12년) 이란의 스캔이글 드론 역설계[12]
- ('14~'17년) ISIS의 이라크 및 시리아 내 미국 무기 탈취[13]
- ('19년) 예멘, 후티 반군의 미국 무기 포획[14]
- ('22년) 우크라이나에서 러시아군의 미국 장비 포획[15,16]

2. 안티탬퍼링 기술

가. 안티탬퍼링 개요

안티탬퍼링은 시스템 또는 기기의 무단 변조를 방지하고, 변조 시도를 탐지하여 적절히 대응하는

보안 기술이다. 이는 물리적, 전자적, 소프트웨어적 수단을 포함하여 시스템의 무결성과 기밀성을 유지하는 데 중요한 역할을 한다.

미국 국방성에 따르면, 안티탬퍼(Anti-Tamper)는 방위 시스템의 중요 프로그램 정보(CPI)의 악용을 방지하거나 지연시키기 위한 시스템 엔지니어링 활동을 포함한다. 이러한 활동은 연구, 설계, 개발, 구현 및 테스트를 포함한 시스템 획득의 전체 수명 주기를 다룬다. 안티탬퍼링의 목적은 역공학, 악용 또는 시스템이나 시스템 구성요소에 대한 대응책 개발을 억제하는 데 중점을 둔다[17].

안티탬퍼링은 SW와 HW를 통해 구현될 수 있다. SW 방식은 코드 난독화, 암호화 및 전자 서명 등이 있고, HW 방식은 물리적 보호를 위한 침입 감지 센서, 특수 보호 케이스 및 TPM을 활용한 암호화 및 키 관리, 펌웨어 보호 및 장치 무결성 검증 등이 있다.

안티탬퍼링은 분실, 불법적 탈취뿐만 아니라 합법적 수출 이후, 시스템에 적용된 최첨단 기술이 비인가자에 의한 역공학, 위변조 공격을 방지하기 위한 기술로, 특히 수출용 방산 무기체계에 가장 시급히 적용해야 할 기술이다.

나. 무기체계 보호 개념

안티탬퍼링은 SW와 HW를 통한 단순 기술 적용 또는 요구 목적에 따라 여러 기술을 조합하여 구현할 수 있으며, 요구 목적 측면에서 개념적으로 표 1과 같이 지연(Deter), 방해(Impede), 탐지(Detect), 반응(Respond)으로 구분할 수 있다[17,18].

표 1 목적에 따른 안티탬퍼링 기술 분류

구분	효과	기술 예시
지연	변조 시간 연장, 탐지 및 대응 시간 확보	물리적 봉인, 보안 테이프, 강화된 케이스
방해	변조 시도 물리적 방해, 성공 가능성 감소	TPM 암호화, 변조 방지 코팅, 감지 센서
탐지	실시간 변조 시도 발견, 조기 대응 가능	침입 탐지 시스템, 변조 감지 센서, 보안 로그 분석
반응	즉각적인 대응, 시스템 무결성 보호	실시간 모니터링, 시스템 종료, 경고 발생

Ⅲ. TCG TPM

1. TCG/TPM/TSS 개요

TCG는 컴퓨팅 기술의 신뢰성을 위해 TPM과 TSS 표준을 개발하는 국제 표준화 기구로 HW 및 SW의 상호 운용성과 보안성을 보장한다.

TPM는 시스템의 무결성과 기밀성을 보장하는 HW 보안 모듈로 암호화 키를 안전하게 저장하고, 시스템 부팅 시 무결성을 검증하며, 무단 접근 시도를 탐지하고 방어하는 기능을 수행한다.

TSS는 TPM 기능을 활용해 보안 서비스를 제공

표 2 TPM 규격 개발 참여사

회사명(기여자 수)	
ANSSI (1)	Lenovo (1)
AMOSSYS (1)	Microsoft (17)
AMD (6)	MIT (1)
ARM Ltd. (1)	MITRE (1)
Atmel (3)	M-Systems Flash (1)
Broadcom (2)	NIST (1)
BSI (2)	Nationz (3)
Certicom (1)	Nokia (1)
CESG (2)	NTRU (3)
Cisco (3)	Nuvoton(4)
Dell (2)	NVIDIA (1)
DMI (1)	Oracle (2)
Fraunhofer SIT (2)	Phoenix (1)
Freescale	PrimeKey Solutions (1)
High North (1)	Safenet (2)
Hewlett Packard (5)	Semiconductor (1)
IBM (1)	STMicroelectronics (4)
Infineon (7)	Symantec (1)
Intel (9)	Thales (1)
ITE (1)	University of Birmingham (1)
Johns Hopkins APL (1)	US Department of Defense (4)
	VIA (1)
	Vodafone (1)
	Wave Systems (3)

하는 소프트웨어 계층으로 다양한 운영체제와 HW 플랫폼에 적용하여, 상호 운용성을 보장한다.

TPM 2.0 표준 규격 개발에 주요 TPM 칩 제조사 및 SW 플랫폼 개발사 등을 포함한 약 45개 사, 100명 이상의 개발자가 기여했다.

표 2는 참여사와 개발자 수를 정리한 것으로, 미국 국방성에서도 4명이 참여한 것을 알 수 있다.

2. TPM 개요

가. 주요 컴포넌트 및 기능

TPM 컴포넌트는 그림 1과 같이, 암호처리, 휘발성 저장소 및 비휘발성 저장소로 구분된다.

1) 암호처리

- 난수 생성기: HW 기반의 난수 생성기는 예측 불가능한 난수를 생성해, 암호화 키와 보안 토큰 생성에 사용된다.
- 키 생성기: 난수 생성기를 통해 비도가 높은 암호화 키를 생성하고, 다양한 암호화 알고리즘에 활용한다.
- 해시 계산기: 데이터를 해싱하여 고유한 해시값을 생성하여 데이터 무결성을 검증하거나 전자서명을 생성할 때 사용한다.
- 암복호화 엔진: (비)대칭 암호화 알고리즘을 지원하며, 데이터의 기밀성과 무결성을 보장한다.

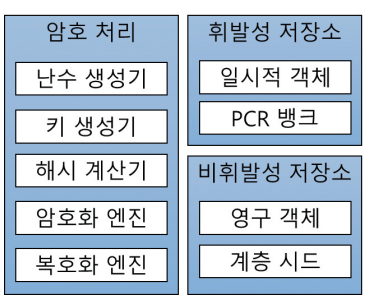

그림 1 TPM 컴포넌트

2) 휘발성 저장소

전원이 꺼지면 데이터가 사라지는 메모리로, 일시적인 데이터 저장에 사용한다.

- 일시적 객체: 임시로 생성되는 암호화 키 또는 인증 토큰 등을 저장한다.
- PCR(Platform Configuration Registers): 시스템의 현재 상태나 설정 정보를 저장하여 부팅 과정에서 시스템 무결성을 검증한다.

3) 비휘발성 저장소

전원이 꺼져도 데이터를 유지하는 메모리로, 중요한 데이터를 영구적으로 저장한다.

- 영구 객체: 영구적으로 저장되는 암호화 키, 인증서 등을 저장한다.
- 계층 시드: TPM의 보안 계층 구조를 정의하는 시드 값을 저장하여 키 계층 구조를 관리한다.

나. TPM 1.2 vs 2.0

TPM 2.0은 TPM 1.2의 SHA-1 알고리즘의 보안 취약성 문제를 개선하고, 다양한 암호화 알고리즘과 새로운 인증 방식을 지원하기 위해 도입되었다[19].

TPM 2.0은 기존 TPM 1.2의 RSA와 SHA-1 대신 RSA, ECC, SHA-2 등 다양한 암호화 알고리즘을 지원하며, 단일 계층(Storage) 대신 다중 계층 구조(Platform, Storage, Endorsement)를 제공한다. 또한, TPM 1.2의 HMAC, PCR, Physical Presence 기반 인증에서 패스워드, HMAC, 정책 기반 인증을 지원한다(표 3 참고).

다. TPM 칩 유형

보안 요구사항과 적용 환경에 따라 표 4와 같이 다양한 형태로 제공된다[20].

표 3 TPM 1.2 vs TPM 2.0

주요 항목	TPM 1.2	TPM 2.0
필수 암호화 알고리즘	RSA-1024, RSA-2048, SHA-1 (해싱 및 HMAC)	RSA-2048, ECC-P256, ECC-BN256, AES-128, SHA-1, SHA-2 (해싱 및 HMAC)
옵션 암호화 알고리즘	AES-128, AES-256	RSA-1024, AES-256
지원 계층 구조	단일 계층 구조 (Storage)	다중 계층 구조 (Platform, Storage, Endorsement)
지원 키 종류	하나의 루트 키 제공 (SRK, RSA-2048)	계층당 여러 루트 키 및 알고리즘 제공
인증 방식	HMAC, PCR, Physical Presence 기반	Password, HMAC, Policy 기반

- Discrete TPM: 전용 칩 형태로, 물리적 공격에 대한 최고 수준의 보안을 제공한다.
- Integrated TPM: 보안 외 기능을 하는 다른 칩과 통합된 형태로 소프트웨어 버그에 강인하지만 물리적 탬퍼 방지 기능은 없다.
- Firmware TPM: TEE(Trusted Execution Environment) 내에서 실행되는 보호된 SW로 TEE OS 또는 응용 버그에 취약할 수 있다.
- Software TPM: SW 에뮬레이터 형태로, TPM 하드웨어 없이 프로토타이핑과 테스팅을 위한 개발 용도로 사용된다.

표 4 TPM 칩 유형 및 특징

유형	보안 수준	보안 특징	비용	응용분야
독립형	최고	탬퍼방지 HW	$$$	크리티컬 시스템
통합형	높음	HW	$$	게이트웨이
펌웨어	높음	TEE	$	엔터테인먼트 시스템
SW	N/A	N/A	¢¢	테스팅 & 프로토타이핑
가상	높음	하이퍼바이저	¢	클라우드 환경

- Virtual TPM: 하이퍼바이저에서 제공되어 가상 머신에서 TPM 기능을 수행한다.

3. TPM 규격 및 프로파일

TCG는 TPM Software Stack(TSS)과 PC, 모바일, 임베디드, 가상화 플랫폼 등 다양한 플랫폼에서 TPM을 구현하는 방법을 설명하는 별도의 규격을 제공한다.

가. TPM 규격서

TPM 규격은 4개 파트(Architecure, Structure, Commands, Supporting Routines)로 구성되며[21], JTC1은 2015년 TCG TPM 2.0 라이브러리 규격의 각 파트를 아래와 같은 ISO/IEC 표준으로 승인했다. 국제표준으로 승인했다.

- (ISO/IEC 11889-1:2015) Part 1: Architecture
- (ISO/IEC 11889-2:2015) Part 2: Structures
- (ISO/IEC 11889-3:2015) Part 3: Commands
- (ISO/IEC 11889-4:2015) Part 4: Supporting Routines

나. TPM 프로파일

TPM은 다양한 목표 제품의 보안성 강화를 위해 특화된 보호 프로파일을 제공한다.

- Protection Profile Automotive-Thin Specific TPM: 자동차 산업의 특수 요구를 충족하기 위해 설계된 표준으로, 차량용 TPM 장치들이 충족해야 할 기준을 정의한다[22].
- Protection ProfilePC Client Specific TPM: 데스크탑 및 노트북에서 TPM 구현과 사용에 대한 세부 사항을 제공한다[23].
- TCG Mobile Reference Architecture: 스마트폰 및 태블릿과 같은 모바일 기기용 TPM 참조 구현

을 제공한다[24].

4. TPM 기능 활용 사례

가. Intel TXT

Intel TXT(Trusted Execution Technology)는 마이크로프로세서의 HW 기반 신뢰 체인을 제공하여 부팅 시점부터 운영체제 및 응용에 이르기까지 시스템을 보호한다[25].

정적 신뢰 기반 측정(SRTM)과 동적 신뢰 기반 측정(DRTM)을 통해 부팅 및 운영체제 실행 중 신뢰 환경을 구축한다. 인증된 코드 모듈(ACM)로 HW 및 SW 구성을 검증하며, GETSEC 명령을 통해 신뢰된 부팅 환경으로 진입 및 종료하는 절차를 갖는다.

- 시스템 초기화: 전원 켜짐 후 CPU가 BIOS를 통해 초기화된다.
- SRTM: BIOS가 시스템 초기 상태를 측정하고 TPM의 PCRs에 저장한다.
- DRTM: 운영체제 부팅 후 GETSEC[SENTER] 명령어로 현재 상태를 측정하고 TPM에 저장한다.
- ACM: Intel의 개인 키로 서명된 모듈을 실행하여 하드웨어 레지스터의 공용 키와 일치하는지 검증한다.

Intel TXT는 TPM을 사용하여 하드웨어 수준에서 시스템의 무결성을 검증하여 보안 실행환경을 제공한다. 한편, Intel PTT(Platform Trust Technology)는 별도의 TPM 하드웨어 없이 펌웨어로 구현한 기술이다. PCR 또는 NV 인덱스를 사용하여 무결성을 보장한다.

나. ARM TrustZone

ARM TrustZone[26]은 SoC 기반 가상 보안 프로세서를 생성하여 보안 세계(Secure World 또는 Trusted Execution Environment)와 일반 세계(Normal World 또는 Rich Execution Environment)를 구분하여 병렬로 운영한다.

NS(Non-Secure) 비트를 통해 메모리와 주변 장치를 보안 세계와 일반 세계로 구분하고, 모니터 모드와 보안 모니터 호출(SMC) 명령어로 보안 모드와 일반 모드 간 전환 관리한다.

HW 기반 보안 분리로 SW에 의존하지 않는 보안 보장을 제공하며 보안 절차는 다음과 같다.

- 시스템 초기화: 전원이 켜지면 ARM 프로세스가 일반 모드와 보안 모드를 초기화한다.
- 보안 설정: NS 비트를 통해 메모리와 주변 장치를 보안 세계와 일반 세계로 구분한다.
- 모니터 모드 전환: SMC 명령어를 통해 일반 모드와 보안 모드 간 전환을 관리한다.
- 보안 세계 작업 수행: 민감한 데이터를 처리하고 암호화 키 관리 등의 작업을 수행한다.
- 보안 세계와 일반 세계 간 통신: 모니터 모드를 통해 데이터 전송을 관리한다.

fTPM은 전용 TPM HW 없이도 격리된 보안 세계(Secure World)를 통해 TPM 기능을 구현할 수 있다.

다. AMD Secure Technology

AMD Secure Processor(구, PSP: Platform Security Processor)[27]는 플랫폼의 메인 코어 프로세서와 독립적으로 실행되는 전용 HW 보안 서브시스템이다.

32비트 마이크로컨트롤러와 온칩 ROM 및 SRAM을 사용하여 보안 코드를 저장하고, 암호화된 DRAM, 암호화 전담 프로세스(CCP), 난수 생성기를 통해 보안 기능 제공한다.

- 시스템 초기화: 전원이 켜지면 AMD Secure Processor(ASP)가 초기화 과정을 수행한다.

- 하드웨어 검증 부트(HVB): ASP가 BIOS의 무결성을 검증한다.
- 신뢰의 루트 확립: SKINIT 명령어로 보안 로더(SL)를 실행하여 신뢰 루트를 구축한다.
- 암호화 기능 수행: 메모리(Secure Memory Encryption)와 가상화 공간(Secure Encrypted Virtualization)을 암호화한다.

ASP는 AMD 칩에 통합된 작은 마이크로컨트롤러로 무결성 측정 값과 암호키를 저장하여, 안전한 부팅, 암호화 및 증명 등 TPM 기능을 구현한다.

Ⅳ. TPM 지원 소프트웨어 스택

1. TCG TSS 개요

TPM Software Stack(TSS)은 TPM과 직접 상호작용하여 보안서비스를 제공하는 소프트웨어 계층이다. TCG TSS 규격은 인텔에 의해 주도적으로 개발되었으며, 그림 2와 같은 API 규격들로 구성된다[4].

TCG TSS는 다양한 응용 분야의 요구사항을 범용적으로 수용할 수 있도록 3개의 계층으로 나누어 개발자 라이브러리를 지원하며, 각각의 특징은 표 5와 같다.

그림 3은 TCG TSS 규격을 지원하는 리눅스 기반 소프트웨어 스택으로 Crypto 및 (Un)Marshalling 등

표 5 TCG TSS 계층별 API 비교

항목	SAPI	ESAPI	FPI
설계 개념	TPM 명령어 직접 접근	SAPI 확장 및 추상화	사례 기반의 고수준의 추상화
주요 사용자	TPM 전문가, 저수준 프로그래밍 개발자	보안에 민감한 응용 프로그램 개발자	TPM, 보안 기술에 대한 비숙련 개발자
주요 기능	TPM 모든 기능과 1:1 맵핑	세션 및 인증 관리, 복잡한 보안 작업 자동화	자동 키 관리, 암호 프로파일 관리, 정책 기반 보안 설정
구현 복잡성	높음	중간	낮음
추상화 수준	낮음	중간	높음
장점	TPM 모든 기능 접근, 유연성, 성능	SAPI보다 사용 간단	사용 간편, 빠른 개발
단점	구현 복잡도, 전문성 요구	TPM 명령 이해 필요	세부 제어 제한

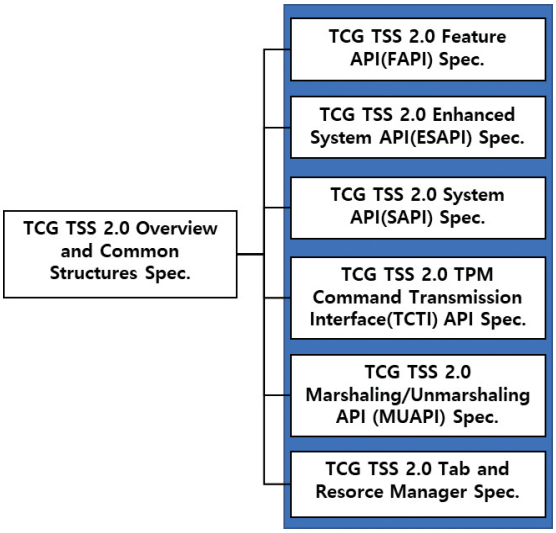

그림 2 TCG TSS 2.0 규격

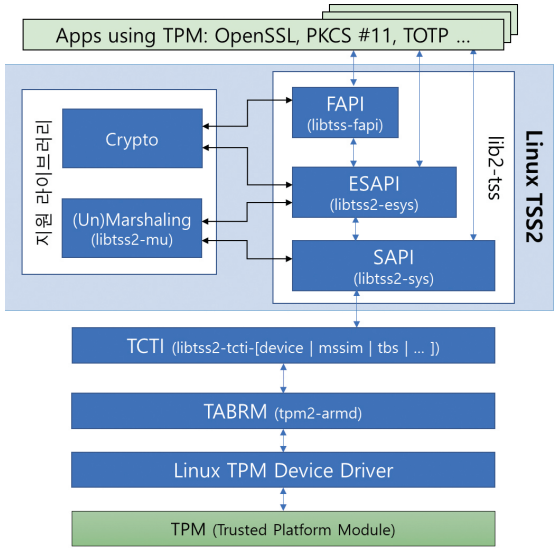

그림 3 Linux TPM 2.0 Software Stack

외부 지원 라이브러리들과 함께 동작할 수 있는 구조로 설계되었다[21].

TCG TSS는 github 사이트를 통한 여러 개의 오픈소스 프로젝트들로 구현된다[28].

tpm2-tss 프로젝트는 TCG TSS의 FAPI, ESAPI, SAPI, (Un)Marshalling, TCTI의 구현으로 libtss2-fapi, libtss2-esys, libtss2-sys, libtss2-mu 등의 라이브러리를 제공한다[29].

tpm2-abrmd 프로젝트는 TAB/RM 기능을 데몬 프로세스로 구현한 것으로, 신규 기능 테스트 및 검증 목적으로 사용된다[30]. TAB/RM은 리눅스 4.12 이후 버전에서 커널 안에 구현되어 기존 데몬 프로세스와 동일한 기능을 제공한다.

가. FAPI

Feature API는 TPM 2.0의 복잡성을 추상화한 상위 계층 API로, 암호화나 TPM에 대한 전문 지식이 없는 사용자도 사용할 수 있으며, 일반적인 사용 사례를 기반으로 약 80%의 응용들을 지원할 수 있다.

- 암호 프로파일과 정책 언어: 다양한 프로파일 제공과 JSON 기반 정책 설정을 지원하여 유연하고 사용자 친화적이다.
- 키 저장 자동화: 사용자의 직접적 관여 없이 안전하게 키를 저장하고 관리한다.
- 사용자 인터페이스 간소화: TPM의 세부적인 데이터 구조를 이해하지 않고도 JSON 인터페이스를 통해 데이터를 관리할 수 있다.

해당 규격은 TSS 2.0 Feature API spec v0.94와 TSS 2.0 JSON Data Types and Policy Language Spec v0.7로, ’20년 6월에 발표되었다.

나. ESAPI

Enhanced System API는 FAPI보다는 복잡하지만 SAPI보다 추상화된 형태로, 암호화 작업이 필요한 응용 프로그램에서 컨텍스트와 세션 관리를 지원한다. 여전히 TPM 2.0에 대한 심층적 이해가 요구되며, 보안이 중요한 C언어 기반 응용 프로그램에 사용된다.

- TPM 전체기능 접근: TPM2의 모든 기능과 HMAC 계산, 암호화/복호화 등 유틸리티 기능을 제공한다.
- 세션 관리 및 상태 유지: HMAC 세션과 암호화된 세션을 자동화하여 상태 유지한다.
- 자동화 처리: 데이터 포맷 변환과 메모리 할당을 자동화하여 안정성을 향상한다.
- 암호 라이브러리 확장성: libgcrypt, OpenSSL 등 외부 암호 라이브러리를 확장 사용하여 기능 및 보안을 강화한다.

다. SAPI

System API는 TPM 2.0의 모든 기능에 대해 1:1 저수준 접근을 제공하는 인터페이스로, 펌웨어 및 BIOS 개발에 적합하며, TPM 및 보안에 대한 전문 지식이 요구된다.

- TPM 명령 변환: C 언어 데이터 타입을 TPM 명령 버퍼로 변환해 TPM 명령을 구성한다.
- TPM 명령 직접 제어: TPM의 모든 기능을 1:1로 직접 제어할 수 있다.
- 펌웨어 보안 부팅: UEFI 초기화 과정에서 보안 부팅 기능을 구현할 수 있다.
- 임베디드 보안: 마이크로컨트롤러에서 구동하는 보안 기능을 구현하여 데이터 보호와 암호화 키 관리 등을 수행한다.

라. (Un)Mashaling

(언)마샬링은 TPM 통신에서 사용되는 데이터 타입의 변환을 담당한다. C 언어의 데이터 타입을

TPM 장치와 통신할 수 있는 전송 포맷으로 변환하거나, TPM 장치에서 반환된 데이터를 C 언어의 데이터 타입으로 역변환한다.

마. TCTI

TPM Command Transmission Interface(TCTI)는 TPM 명령 및 응답을 바이트열 문자열로 송수신하는 인터페이스로, 다양한 유형의 TPM 장치들과 연결할 수 있는 통신 채널을 제공한다.

- 통신 추상화: 개발자가 IPC 메커니즘의 세부 사항을 몰라도 다양한 플랫폼에서 TPM 기능을 일관되게 사용할 수 있도록 통신 추상화 계층을 제공한다.
- 다양한 통신 채널 지원: TPM과의 통신을 위해 libtss2-tcti-[device|mssim|tbs]와 같은 라이브러리 모듈을 제공한다. 여기서. *-device는 실제 TPM 장치와 통신, *-mssim은 개발 및 테스트 목적으로 Microsoft의 TPM2 시뮬레이터와 통신, *-tbs는 Windows에서 TPM Base Services와 통신하는 데 각각 사용된다.

바. TAB / RM

TPM Access Broker는 다중 프로세스 간 TPM 자원을 효과적으로 관리하고 동기화 처리를 담당한다. Resource Manager는 제한된 메모리 환경에서 필요에 따라 개체, 세션 및 시퀀스 등을 스왑(Swap)시켜 메모리 사용을 최적화한다.

2. 기타 TSS 오픈 소스 구현

인텔 주도의 TCG TSS 외에도 IBM TSS[31], WolfTPM[32,33], TPM-JS[34] 등 TPM 2.0 표준 규격을 지원하는 다양한 오픈소스 프로젝트가 존재한다(그림 4 참고).

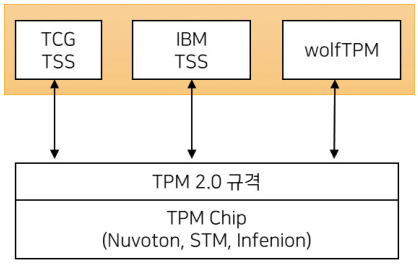

그림 4 TPM 2.0 규격 지원 TSS

가. IBM TSS

TPM 2.0 명령을 실행할 수 있는 간단한 인터페이스를 제공하며, 이는 TCG TSS의 여러 계층(ESAPI, SAPI 및 TCTI) 기능과 동등하다. 이 구현에는 스크립트 앱, 프로토타이핑, 교육 및 디버깅에 사용할 수 있는 110개 이상의 TPM 도구 샘플이 포함되어 있다.

IBM TSS의 API는 'TSS_Execute'라는 단일 함수를 통해 모든 TPM 2.0 명령을 호출하며, 이 명령들은 매개변수 코드 'TPM_CC'를 통해 처리되는 일관된 인터페이스를 제공한다.

IBM TSS는 사용자로부터 숨겨진 방식으로 다음을 처리한다.

- HMAC, 비밀번호 및 정책 세션
- 바인드(Bind) 및 솔트(Salt) 세션을 포함한 세션 키 및 HMAC 키 계산
- HMAC 생성 및 검증
- 매개변수 암호화 및 복호화, XOR 및 AES
- 논스 및 논스 롤링
- 세션 계속 플래그
- TPM 2.0 "이름" 및 바인드 세션 추적
- 다양한 세션 해시 알고리즘
- (언)마샬링 및 TPM과의 통신

속성값(Properties)을 통해 연동될 TPM 장치 유형과 디버깅 수준 등의 실행 환경을 설정할 수 있

다. 지원되는 장치 유형은 리눅스 커널 디바이스 및 TPM 시뮬레이터가 포함된다. 이 설정은 응용 프로그램 시작 시 셸 환경변수를 통해 지정되며, TSS_SetProperty() 함수를 통해 런타임 중에 변경 가능하다.

나. WolfTPM

WolfSSL에서 제공하는 오픈소스 기반의 경량 TPM 소프트웨어 스택으로, 임베디드 시스템 및 IoT 기기에 최적화되어 낮은 리소스 소비와 높은 성능을 제공한다.

WolfTPM은 TPM2와 래퍼(Wrapper) 계층의 API로 구성된다. TPM2 API는 TPM 2.0 표준을 준수하는 명령과 데이터 구조체 관리를 담당하며, 래퍼 API는 키 생성/저장, 증명(Attestation), 매개변수 암호화 같은 보다 상위 개념의 기능을 사용하기 쉽게 설계되었다. WolfSSL[35]라는 외부 라이브러리를 활용하여 자격부여 세션 처리와 매개변수 암호화를 수행한다.

- TPM 2.0 규격을 준수하는 모든 TPM 2.0 API를 제공한다.
- 키 생성, NV 메모리, RSA 암복호화, ECC 서명/검증, ECDH 등 일반적인 사용 사례를 위한 래퍼를 제공한다.
- 증명(Attestation), 인증서 서명 요청(CSR), 서명된 타임스탬프 생성(TPM 2.0 GetTime) 등 고급 사용 사례에 대한 예제를 제공한다.
- Windows 및 Linux를 지원하며 이식성이 높아 RTOS 응용 또는 펌웨어 일부로 동작할 수 있다.

다. TPM-JS

TPM-JS[34]는 자바스크립트 환경에서 TPM 기능을 사용할 수 있게 해주는 오픈 프로젝트로, 실제 TPM 장치가 없어도 TPM의 다양한 기능을 시뮬레이션할 수 있어 학습과 실험에 매우 유용한 도구다.

TPM-JS는 내부적으로 Google BoringSSL(SSL/TLS 구현하는 오픈 소스 라이브러리), IBM TPM2 Simulator (실제 TPM 하드웨어 동작을 시뮬레이션), Intel TPM2 TSS(TCG TSS 2.0 지원 라이브러리)를 포함한다. 이를 활용하면 웹 브라우저 및 Node.js 환경에서 TPM의 보안 기능을 사용하여, 웹 응용 프로그램의 보안을 강화할 수 있다.

Ⅴ. 무기체계 기술 보호 연구 동향

1. 안티탬퍼링 기술 개발 동향

국내에서는 핵심기술 연구개발 사업 및 방위산업 육성 지원사업 형태로 수행되고 있다[36].

국방기술진흥연구소의 무기체계 기술 보호 기법('22~'26년) 패키지형 과제에서는 ETRI, LIG넥스원, 쿤텍 등이 참여하여, 다양한 무기체계에 보드/칩, 코드, SW 수준에서 적용할 수 있는 안티탬퍼링 기술을 개발 중이다[37].

국방과학연구소는 무기체계 S/W플랫폼 안티탬퍼링 기술('19~'23년) 과제를 통해 여러 무기체계에 공통으로 활용할 수 있는 탬퍼링 감지, 차단 및 관련 도구 개발을 포함하는 연구개발을 진행하였다[38]. 또한, 국방과학연구소는 무기체계 안티탬퍼링 적용 기술('22~'26년) 과제에서 탬퍼링 차폐, 부채널 분석 방지, 임베디드 시스템 TEE 적용 기술을 통해 파괴적/비파괴적 탬퍼링에 대응하는 연구를 진행 중이다[39].

2. 방산 기술 보호 규제 및 기준

방위사업청 주도로 수출 무기체계의 핵심기술 보호를 위해 안티탬퍼링 기술 적용 의무화 정책을 강화하고 있다.

- 수출 무기체계 안티탬퍼링 적용 및 전담 조직 신설 제시(방위산업기술보호 시행계획, 방위사업청 국방기술보호국, '22. 12.)
- 안티탬퍼링 기술 관리체계 구축 노력(안티탬퍼링 관리체계 구축 추진 계획(통보), 방위사업청 기술보호과-1090, '23. 3.)
- 수출 무기체계에 안티탬퍼링 기술 적용 의무화(방위산업기술 보호지침, 개정 '23. 5.)

VI. 결론

무기체계 기술 보호는 국가 안보를 유지하는 데 필수적이다. 최근 AI 기술의 발전과 글로벌 방산 시장에서 한국의 위상변화는 안티탬퍼링 기술의 중요성을 더욱 부각시킨다. 이러한 환경에서 TPM 기반 안티탬퍼링 기술은 무기체계의 무결성과 기밀성을 보장하는 중요한 도구로 활용될 수 있다.

본고에서는 안티탬퍼링의 정의와 필요성, 기술 유출 사례를 살펴보고, TPM 표준 현황, TPM 기반 소프트웨어 스택 구현을 위한 글로벌 오픈 프로젝트 기술 동향을 분석했다.

향후, 수출 무기체계의 방산 기술 보호를 위해 안티탬퍼링 기술이 의무적으로 탑재될 예정이므로 저비용 대비 고수준의 보안성을 제공하는 TPM 기반 안티탬퍼링 솔루션이 K-방산 기술의 효과적인 보호 수단을 제공할 수 있을 것이다.

용어해설

Anti-Tampering 시스템이나 기기의 무단 변조를 방지하고, 변조 시도를 탐지하며 이를 적절히 대응하는 보안 기술

TPM 시스템의 무결성과 기밀성을 보장하는 HW 기반 보안 모듈

TSS TPM과 상호작용하는 SW 계층으로, TPM의 기능을 활용하여 보안 서비스를 제공

TCG 컴퓨팅 기술의 신뢰성을 보장하기 위해 다양한 표준을 제정하는 국제 표준화 기구

약어 정리

ACM	Authenticated Code Module
AMD	Advanced Micro Devices
ARM	Advanced RISC Machine
AT	Anti-Tamper(ing)
BIOS	Basic Input/Output System
CPI	Critical Program Information
CSR	Certificate Signing Request
DRTM	Dynamic Root of Trust for Measurement
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ESAPI	Enhanced System API
FAPI	Feature API
HMAC	Hash-based Message Authentication
HVB	Hardware Verified Boot
IPC	Inter-Process Communication
MUM-T	Manned-Unmanned Teaming
NV	Non-Volatile
PCR	Platform Configuration Register
RM	Resource Manager
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SAPI	System API
SHA-1	Secure Hash Algorithm-1
SMC	Secure Monitor Call
SRK	Storage Root Key
SRTM	Static Root of Trust for Measurement
SSL	Secure Sockets Layer
TAB	TPM Access Broker
TCG	Trusted Computing Group
TCTI	TPM Communication Transmission Interface
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSS	TPM Software Stack
TXT	Trusted Execution Technology
UEFI	Unified Extensible Firmware Interface

참고문헌

[1] 국방부, "국방혁신 4.0," 2023. 2. 28.

[2] TCG, https://trustedcomputinggroup.org

[3] TCG, TPM 2.0 Library Specification

[4] TCG, TSS 2.0 Overview and Common Structures Specification

[5] 배성은, "세계를 뛰어넘을 K-방산 전략," 아주경제, 2023. 11. 19.

[6] 삼일PwC경영연구원, "W.E.A.P.O.N: 키워드로 보는 방위산업의 현재와 미래," Industry Focus, 2024. 7.

[7] 국방기술진흥연구소, "AI 기반의 유·무인 복합전투체계 발전을 위한 제언," 이슈페이퍼, 제9호, 2023.

[8] 국방기술진흥연구소, "유·무인 협업체계(MUM-T) 기술수준 평가," 이슈페이퍼, 제5호, 2022.

[9] G. Cohen, "Chinese Hackers Steal U.S. Fighter Jet Plans," The Wall Street Journal, 2014. 1. 22.

[10] BBC News, "Iran Shows Off Alleged Downed US Drone." 2011. 12. 8.

[11] Al Jazeera, "Iran Says It Hacked U.S. Drone, Shows Video," 2011. 12. 12.

[12] B. Lendon, "Iran Claims It Captured, Copied US Drone," CNN, 2012. 12. 17.

[13] The Hill, "ISIS Seized More Than 2,300 Humvees from Iraqi Forces," 2015. 5. 31.

[14] Reuters, "Yemen's Houthis Seize U.S.-Made Weapons from Saudi-Led Coalition," 2019. 7. 19.

[15] The New York Times, "Russia Captures U.S.-Supplied Weapons in Ukraine," 2022. 3. 1.

[16] I.S. Bisht, "Russia Traded Captured Western Weapons for Iranian Drones: Report," The Defense Post, 2022. 11. 9.

[17] What is Anti-Tamper-U.S. Department of Defense, https://at.dod.mil/What-Is-Anti-Tamper

[18] 이민우 외, "무기 시스템 개발에서 기술보호를 위한 위험관리 기반의 Anti-Tampering 적용 기법," 제19권 제12호, 2018, pp. 99-108.

[19] W. Arthur, D. Challener, and K. Goldman, "A Practical Guide to TPM 2.0," Springer, 2015.

[20] TCG, "TPM 2.0: A Brief Introduction," 2019. 6.

[21] TCG, "Trusted Platform Module Library Part1: Architecture," 2014. 10.

[22] TCG, "Protection Profile Automotive-Thin Specific TPM," Level 0 Ver. 1.0, 2018. 12.

[23] TCG, "Protection Profile PC Client Specific TPM," Ver. 1.3, 2021. 9.

[24] TCG, "TCG Mobile Reference Architecture," Ver. 2.45, 2023. 8.

[25] Intel Trusted Execution Techonology(TXT), https://www.intel.com/content/www/us/en/developer/articles/tool/intel-trusted-execution-technology.html

[26] ARM TrustZone, https://www.arm.com

[27] AMD Secure Processor, https://www.amd.com

[28] https://github.com/tpm2-software

[29] https://github.com/tpm2-software/tpm2-tss

[30] https://github.com/tpm2-software/tpm2-abrmd

[31] https://sourceforge.net/projects/ibmtpm20tss

[32] https://www.wolfssl.com/products/wolftpm

[33] https://github.com/wolfSSL/wolfTPM

[34] https://google.github.io/tpm-js

[35] https://github.com/wolfSSL/wolfssl

[36] 방위사업청, '23-37 국방기술기획서, 2023. 5.

[37] 방위사업청, "무기체계 기술보호기법," 국방기술진흥연구소(RFP), https://www.ntis.go.kr

[38] 방위사업청, "무기체계 소프트웨어 플랫폼 안티탬퍼링 기술," 국방기술진흥연구소(RFP), https://www.ntis.go.kr

[39] 국방기술진흥연구소, "무기체계 기술 보호를 위한 안티탬퍼링 적용 방안 제언," 이슈페이퍼, 제10호, 2023.