무기체계 하드웨어 안티탬퍼 기술
- PCB를 대상으로 -

Anti-tamper Technology for Weapon Systems Hardware
- Focusing on PCB -

주영진*,1) . 김태현2) . 손창근1) . 송경호1) . 류연승3) . 이규호4) . 배영채4)

Youngjin Joo*,1) . TaeHyun Kim2) . Changgun Son1) . Kyungho Song1) . Yeonseung Ryu3) . Kyuho Lee4) . Youngchae Bae4)

[초 록]

최근 무기체계의 수출이 증가하면서 수출된 무기체계에 구현된 핵심기술이 수입국의 역공학(reverse engineering) 공격을 통해 탈취될 위험도 증가하고 있다. 무기체계에 구현된 핵심기술 중에서 컴퓨터 하드웨어 및 소프트웨어로 구현된 기술은 역공학 기법을 사용하여 탈취가 매우 용이하다. 소프트웨어 수준에서는 대부분 코드 난독화, 암호화 기법 등의 역공학 대응 기술을 적용하고 있지만 하드웨어 수준에서 역공학 대응 기술의 적용은 미미하다. 본 논문은 하드웨어 중에서도 PCB(Printed Circuit Board)를 대상으로 역공학 대응을 위한 안티탬퍼(anti-tamper) 기술들을 조사하였다. 이러한 기술 조사를 바탕으로 여러 무기체계에 공통으로 적용하는 안티탬퍼 기술의 표준화에 기여할 수 있다.

[ABSTRACT]

With the recent increase in exports of weapon systems, the risk of core technologies implemented in these systems being stolen through reverse engineering attacks by importing countries is also rising. Among the core technologies implemented in weapon systems, those implemented in computer hardware and software are particularly easy to steal using reverse engineering techniques. While most software-level countermeasures against reverse engineering, such as code obfuscation and encryption, are applied, the application of such countermeasures at the hardware level is minimal. This paper investigates anti-tamper technologies for countering reverse engineering, specifically focusing on Printed Circuit Boards (PCBs) within the hardware sector. Based on this technical investigation, this study can contribute to the standardization of anti-tamper technologies applicable to various weapon systems.

Key Words : Weapon System(무기체계), Hardware(하드웨어), Technology Protection(기술보호), Reverse Engineering(역공학), Anti-Tamper(안티탬퍼), PCB(PCB), Chip(칩)

1. 서론

우크라이나-러시아 전쟁 이후 K2 전차, K9 자주포, 천궁, FA-50 훈련기 등 무기체계 수출이 급증하고 있으며 정부는 지속적인 수주 확대를 통해 글로벌 4대 방산 수출국 진입을 목표로 하고 있다. 그러나, 무기체계 수입국들이 핵심기술의 이전, 현지생산 등을 요구하고 있어 막대한 비용을 들여 개발한 국방 핵심기술이 향후 방산 시장에서 경쟁국이 될 수도 있는 나라들에게 쉽게 유출될 위험이 있다. 따라서 수출용 무기체계 핵심기술의 보호를 위한 체계적인 준비가 필요하며 그 중에서 무기체계에 구현된 핵심기술의 역공학 대응도 필요하다.

1) 명지대학교 보안경영공학과
(Department of Security and Management Engineering, Myongji University, Korea)
2) 명지대학교 방산안보학과
(Department of Defense Industrial Security, Myongji University, Korea)
3) 명지대학교 반도체ICT대학 컴퓨터정보통신공학부 컴퓨터공학전공
(Department of Computer Engineering, Myongji University, Korea)
4) LIG D&A 사이버전자전개발팀
* Corresponding author, E-mail: yjj3620@mju.ac.kr

Recived : June 15, 2026 Revised : June 24, 2026
Accteped : June 30, 2026

국방 선진국인 미국은 압도적인 성능의 무기체계로 글로벌 무기체계 시장의 약 50%를 점유하고 있으며, 군사적 우위를 유지하기 위해 자국의 핵심기술을 다양한 방법으로 보호하고 있다. 이는 프로그램 보호(program protection) 계획의 일부로서 수행되며 그 중에서 안티탬퍼(anti-tamper)는 무기체계에 구현된 핵심 프로그램 정보(CPI: Critical Program Information)를 보호하기 위한 공학적 대책이다. [1] 미국은 안티탬퍼를 단순히 보안 기능을 추가하는 것이 아니라, "무기체계 획득의 전 수명 주기에 걸쳐 핵심 프로그램 정보(CPI)의 악용을 방지하거나 지연시키기 위해 수행하는 시스템 엔지니어링(Systems Engineering) 활동"으로 정의한다. 이는 안티탬퍼 기술이 설계, 개발, 구현, 시험검증 단계에 이르기까지 체계적으로 통합되어야 함을 시사한다.

우리나라는 2015년 방위산업기술보호법이 제정될 때 수립된 종합계획에서 무기체계 '기술보호기법'이란 명칭으로 안티탬퍼를 다루었지만 관련 지침 제정 등의 정책 수립에는 소극적이었다. 최근 수출이 활발해지면서 이미 개발이 끝나고 수출하는 무기체계에 안티탬퍼 적용을 방산업체에 요구하고 있지만 적용이 불가능한 실정이다. 아직까지 미국처럼 여러 무기체계에 공통으로 적용할 기술의 표준이 없고, 보호대상의 중요도, 위험(risk) 수준 등에 따라 규정되는 보호 등급(protection level) 정책도 부재하다. 또한, 안티탬퍼 기술의 성능을 검증할 방법도 정립되어 있지 않다.

무기체계에 구현된 핵심기술 중에서 컴퓨터 하드웨어 및 소프트웨어로 구현된 기술은 다양한 역공학 기법들이 알려져 있어 탈취가 용이하다. 역공학에 대비하기 위하여 소프트웨어 수준에서는 대부분 코드 난독화, 암호화 기법 등의 이미 잘 알려진 안티탬퍼 기술을 적용할 수 있지만 아직까지 하드웨어 수준에서 안티탬퍼 기술의 적용은 고려하지 못하고 있다. 일반적으로 정보시스템의 하드웨어는 칩, PCB(Printed Circuit Board), 패키징(Packaging)의 계층 구조로 이루어져 있다. 이러한 구조에서 역공학 시도는 정보시스템을 감싸고 있는 패키징 해체로 시작하여 PCB 분석, 그리고 최종적으로 칩 내부의 데이터를 추출하는 순서로 진행된다. 따라서 하드웨어의 안티탬퍼 기술은 단일 계층의 보호가 아닌, 이 세 가지 계층 전반에 걸친 다층적 방어 전략으로 구현되어야 한다. 본 논문은 하드웨어 중에서도 PCB(Printed Circuit Board)를 대상으로 역공학 기법과 대응을 위한 주요 안티탬퍼 기술들을 조사하였다. 이러한 기술 조사를 바탕으로 여러 무기체계에 공통으로 적용하는 안티탬퍼 기술의 표준화에 기여할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 안티탬퍼 기술의 유형을 설명한다. 3장에서는 PCB 대상의 역공학 기법을 설명하고 4장에서는 역공학 기법에 대응하기 위한 안티탬퍼 기술을 설명한다. 5장에서는 결론 및 향후과제를 기술하였다.

2. 안티탬퍼 기술 유형

안티탬퍼 기술은 공격 대응 메커니즘과 목적에 따라 억제(Deterrence), 방지(Resistance), 감지(Detection), 반응(Response)의 4가지 유형으로 분류된다. 각 분류별 설명과 예시는 표 1과 같다.

표 1. 안티탬퍼 기술 유형
Table 1. Type of Anti-Tamper technology

유형	설명 및 예시
억제	비인가자의 탬퍼링을 사전에 시도하지 못하도록 하는 방법이나 기술 - Seal 또는 Label을 사용자에게 주의를 환기하여 접근을 차단
방지	비인가자의 탬퍼링을 지연 및 저지, 방해하는 방법이나 기술 - 특수 볼트, 용접, 접착, 코팅 등 - SW 난독화, 암호화 등
감지	비인가자의 접근을 시스템 또는 사용자가 알 수 있도록 하는 방법이나 기술 - 손을 대는 경우 표시가 나거나 파손되는 스티커를 붙여놓는 방법 - 기계/센서적 감시, 인증, 무결성 검증 등
반응	비인가자의 탬퍼링 접근을 인지한 경우, 특정 조치를 수행하는 방법이나 기술 - 데이터 삭제나 장치의 물리적 파괴 등

3. PCB 역공학 기법

3.1 PCB

PCB는 전자 부품을 전기적으로 연결하고 기계적으로 지지하는 부품이다. 구성하는 요소들을 물리적으로 고정하고, 전기적으로 연결하여 전자제품 내부에서 전류와 신호가 이동할 수 있도록 회로가 설계되어 있으며, 반도체, 저항, 커패시터, 커넥터 등의 부품으로 구성 되어있다.

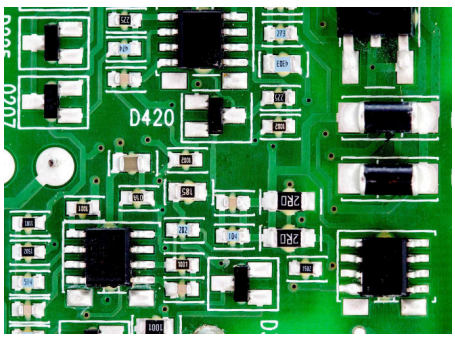

그림 1. PCB (Printed Circuit Board)
Fig. 1. Printed Circuit Board

PCB는 층수(단면, 양면, 다층), 구조(연성, 경성, 복합), 재질(FR-4, 세라믹, 금속)에 따라 종류가 나뉜다. 예를 들어, 층수를 기준으로 다음과 같은 PCB 종류들이 있다.

표 2. PCB의 종류
Table 2. Type of PCB

종류	설명
단면 PCB	한쪽 면에만 회로가 위치하며, 저가형 전자기기에 많이 사용
양면 PCB	앞뒤 양면에 회로가 위치하며, 비아(via)로 연결
다층 PCB	3층 이상 적증 구조로서 고성능/고신뢰성 응용에 많이 사용

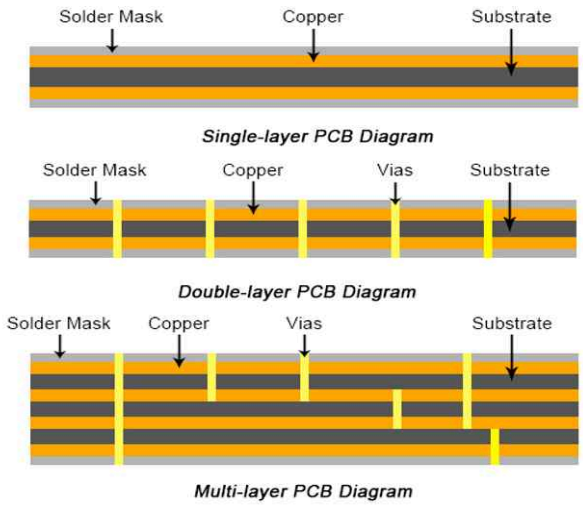

그림 2. PCB의 종류 (출처: Pcbcart)
Fig. 2. Type of PCB (Pcbcart)

3.2 PCB 역공학

PCB 역공학은 일반적으로 그림 3과 같은 단계로 진행되며, PCB의 적층 분해, 스캐너나 x-ray 등을 이용한 이미지 캡처(imaging) 등을 통해 구성품 및 연결을 식별하고, PCB file (Gerber), BOM list, PCB schematics를 획득한다. 이를 통해 보드에 연결된 부품의 정보와 이들 간의 연결 관계를 파악하여 회로도를 복원하는 것을 주된 목적으로 한다. 공격자는 시스템의 동작 원리를 이해하고, 취약점을 식별하여 펌웨어를 추출하거나 복제 보드를 제작할 수 있다.

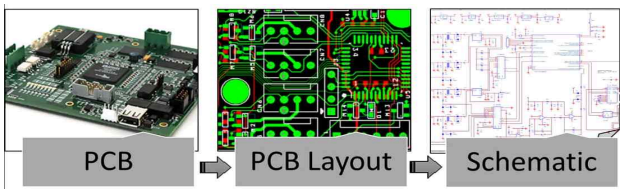

그림 3. PCB 역공학 절차
Fig. 3. PCB reverse-engineering process

PCB 역공학은 파괴적 공격과 비파괴적 공격의 두 유형으로 구분할 수 있으며, 각 세부 공격 방법은 표 3과 같다.

표 3. PCB 역공학 유형
Table 3. Type of PCB reverse engineering

구 분	세부 공격 방법
파괴적 공격	프로빙 (Probing) : 신호 분석, 주입 공격 등
	마이크로 프로빙 (Microprobing) : 데이터 버스 분석, 신호 주입 등
	인터페이스 프로빙: JTAG, UART, SPI, I2C 등 디버깅 및 통신 포트에 분석 장비 연결
	기계적 제거 (Mechanical Removal) : 레이어 분해 (Delayering)
비파괴적 공격	광학 현미경 (Optical Microscopy)
	주사 전자 현미경 (Scanning Electron Microscopy, SEM)
	집속 이온 빔 (Focused Ion Beam, FIB)
	X-선 단층 촬영 (X-ray Computed Tomography, XCT)
	자외선 광자 방출 현미경 (UV Photon Emission Microscopy, PEM)
	적외선 현미경 (Infrared Microscopy)
	전력 및 전자파 분석

3.2.1 파괴적 역공학

다양한 방법으로 PCB에 물리적으로 접근하여 변조, 분석, 공격을 시도하는 기술이다.

- 프로빙: PCB의 신호선, 전력선, 데이터 버스 등에 직접 프로브를 연결하여 전기적 신호를 측정하거나 주입하는 기술이다.
  - 신호 분석: 데이터 라인이나 클럭 신호를 모니터링하여 민감한 정보를 추출함
  - 주입 공격: 전기적 신호를 주입하여 시스템 동작을 방해하거나 의도한 대로 조작함
- 마이크로 프로빙: 매우 작은 프로브를 사용하여 내부 신호를 직접 탐침하는 방법으로 공격자는 매우 정밀한 위치에서 신호를 감지하거나 주입한다.
  - 데이터 버스 분석: 매우 세밀한 데이터 라인을 모니터링하여 중요한 데이터를 캡처할 수 있음
  - 신호 주입: 특정 위치에 신호를 주입하여 시스템의 동작을 변조할 수 있음
- 인터페이스 프로빙: JTAG, UART, SPI, I2C 등 디버깅 및 통신 포트에 분석 장비(Logic Analyzer, Oscilloscope)를 연결한다.
  - 펌웨어를 덤프(Dump)
  - 버스 상의 데이터 패킷을 스니핑(Sniffing)

- 기계적 제거: PCB나 IC의 특정 부분을 물리적으로 제거하여 내부 구조에 접근하는 방법으로 드릴, 밀링 머신, 레이저 커터 등의 도구를 사용하여 수행한다.
  - 층별 분석: PCB의 각 층을 물리적으로 제거하여 내부 회로를 분석하는 기술

3.2.2 비파괴적 역공학

물리적인 손상을 가하지 않고 외부에서 관찰할 수 있는 정보를 수집하는 기법으로 일반적으로 고해상도의 이미지 장비와 고도로 정밀한 분석 도구를 사용한다.

- 광학, 전자빔, 집속 이온 빔, 적외선, 자외선 현미경: 고해상도 카메라 및 현미경을 사용하여 PCB 표면에 노출된 배선(Trace), 비아(Via), 실장 부품의 위치 및 마킹 정보를 수집한다. 이를 통해 주요 부품(MCU, Memory, FPGA 등)을 식별하고 신호 흐름을 분석한다.
- X-선 촬영: 다층 PCB의 경우 내층(Inner Layer)의 배선은 육안으로 확인할 수 없다. 공격자는 X-Ray 장비를 이용하여 내부 배선 구조를 투시 촬영하거나, 3D CT(Computed Tomography) 촬영을 통해 입체적인 배선 연결 정보를 획득한다.
- 전력 및 전자파 분석: PCB의 전원 라인이나 특정 부품에서 방출되는 전자파를 측정하여 내부 동작 상태를 유추하거나 암호키 관련 정보를 획득한다.

4. PCB 안티탬퍼 기술

앞 2장에서 제시한 안티탬퍼 기술 유형 중에서 PCB에 적용할 수 있는 유형로는 물리적 접근을 차단하는 방지 기술, 침입 시도를 인지하는 감지 기술 및 반응 기술이 가능하다.

4.1 방지 기술

4.1.1 물리적 커버

PCB의 내용을 볼 수 없게 하거나 물리적으로 접근하는 것을 어렵게 만드는 기술로 다양한 소재를 이용하여 PCB를 덮는 덮개(Cover)를 만드는 기술 등이 있다.

- 메시 (mesh) : PCB 또는 IC 상에 매우 촘촘한 망을 형성하여 물리적 공격을 방지한다.
- 컨포멀 코팅 (Conformal Coating): 습기나 먼지 방지 수준을 넘어, 불투명하고 제거가 어려운 특수 재질로 PCB 표면을 코팅한다. [9]
- X-Ray 방어: 텅스텐 등 X-Ray 흡수율이 높은 물질을 포팅재에 섞어 내부 회로의 투시 촬영을 방해한다.

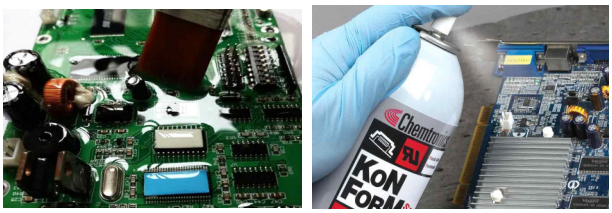

그림 3. PCB 안티탬퍼 물리적 커버 기술

Fig. 3. PCB Anti-tamper physical cover technology

4.1.2 난독화 (obfuscation)

회로가 노출되더라도 그 기능을 쉽게 파악하지 못하도록 혼란을 주는 기술이다.

- 부품 마킹 제거 (De-marking/Re-marking): 레이저나 샌드블라스트를 이용해 칩 패키지 표면의 파트 넘버와 제조사 로고를 지우거나, 엉뚱한 부품 번호로 위장 마킹하여 부품의 기능을 식별하지 못하게 한다.
- 매립형 비아 (Buried/Blind Vias): 신호 배선을 PCB 내층으로만 연결하고(Buried Via), 표면에는 노출시키지 않는 기술이다. 외부에서의 신호 프로빙을 불가능하게 만들고, X-Ray 분석 없이는 신호 경로 추적을 매우 어렵게 한다.
- 더미 요소 삽입 (Dummy Insertion): 실제 동작에는 관여하지 않는 가짜 배선이나 가짜 부품을 배치하여 회로 분석가에게 혼선을 주고 분석 시간을 지연시킨다.

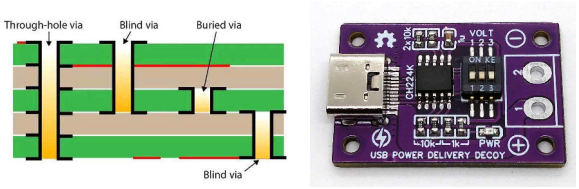

그림 4. PCB 난독화 기술

Fig. 4. PCB obfuscation technology

4.2 감지 기술

공격자의 탬퍼링 시도를 실시간으로 감지하여 시스템의 대응을 유도하는 기술이다.

4.2.1 물리적 침입 감지

공격자가 PCB 내부를 확인하기 위한 탬퍼링 시도로 시스템의 외관이나 구조적 무결성이 훼손되는 것을 감지하는 기술이다.

- 전도성 메시 및 필름 (Conductive Mesh & Film): PCB나 중요 부품을 감싸는 포팅재 내부에 미세한 전도성 패턴을 형성한다. 공격자가 내부 회로에 접근하기 위해 드릴링(Drilling)이나 절단(Cutting)을 시도할 경우, 패턴이 끊어지거나(Open) 합선(Short)되어 저항값이 변하는 것을 감지한다.
- 스위치 및 센서 (Switches & Sensors): 기기의 케이스

(Chassis)가 열리는 순간을 감지하는 마이크로 스위치(Micro-switch)나 리드 스위치(Reed Switch)를 설치한다. 또한, 기기에 가해지는 비정상적인 충격이나 진동을 감지하는 가속도 센서, 케이스 파손 시 내부 압력 변화를 감지하는 압력 센서 등이 활용된다.

- 광 감지 (Light Detection): 불투명한 케이스나 칩 패키지가 파손되어 내부로 빛이 유입되는 것을 감지한다. 주로 포토다이오드(Photodiode)나 조도 센서가 사용되며, 칩 디캡슐레이션 공격을 탐지하는 데 효과적이다.

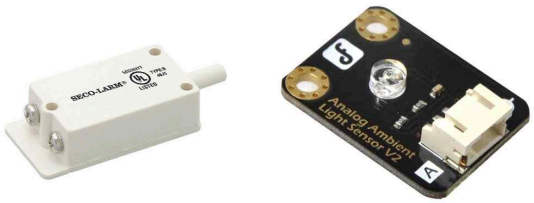

그림 5. 물리적 침입 감지 기술 (좌: 탬퍼 스위치, 우: 광 감지 센서)

Fig. 5. Physical intrusion detection technology (Left: Tamper switch, Right: Optical sensor)

4.2.2 환경적 공격 감지

공격자가 시스템의 오동작을 유도하기 위해 극한의 환경을 조성하거나 신호를 조작하는 행위를 감지하는 기술이다.

- 온도 감지 : 칩의 데이터 잔존(Remanence) 시간을 늘리기 위해 액체 질소 등으로 급속 냉각시키는 '콜드 부트 공격(Cold Boot Attack)'이나, 고온 스트레스를 주어 오류를 유발하는 행위를 감지하기 위해 설정된 임계 온도 범위를 벗어나는지 지속적으로 모니터링하는 기술이다.
- 전압 및 클럭 글리치 감지 (Voltage & Clock Glitch Detectors): 정상 전압 범위보다 낮거나 높은 전압을 순간적으로 주입하거나(Voltage Glitch), 클럭 주파수를 비정상적으로 높이거나 낮추는(Clock Glitch) 오류 주입 공격(Fault Injection)을 탐지하는 기술이다.
- X-Ray 및 이온 빔 감지: PCB 내부 배선이나 칩 회로를 투시하기 위해 조사되는 강력한 X-Ray 선량이나, FIB(집속이온빔) 가공 시 발생하는 이온 농도 변화를 감지하는 특수 센서 기술이다.

4.3 반응 기술

4.3.1 데이터 소거 및 제로화 (Zeroization)

가장 보편적이고 필수적인 대응 기술로, 메모리에 저장된 민감한 데이터(암호키, 인증서, 중요 알고리즘 등)를 삭제하는 것이다.

- 능동적 소거 (Active Zeroization): 프로세서나 보안 컨트롤러가 감지 신호를 받으면 즉시 메모리 영역에 '0' 또는 무작위 패턴을 덮어쓰기(Overwrite)하여 데이터를 복구 불가능하게 만든다. 이 과정은 수 마이크로초(μs) 또는 나노초(ns) 단위의 매우 짧은 시간 내에 완료되어야 한다.
- 전원 차단: 배터리로 데이터가 유지되는 RAM의 경우, 배터리 연결 회로를 물리적으로 끊어버림으로써 램의 휘발성(Volatile) 특성을 이용해 데이터를 즉시 증발시킬 수 있다.

4.3.2 물리적 파괴

최고 등급의 보안이 요구되는 무기체계나 핵심 모듈의 경우, 하드웨어 자체를 물리적으로 파괴하는 강력한 대응이 적용된다.

- 온-칩 소각 (On-chip Destruction): 칩 내부에 고전압을 인가하여 트랜지스터 게이트를 태워버리거나, 과전류를 흘려 구성요소를 영구적으로 불능상태로 만드는 기술이다.
- 기폭 및 자폭 장치: 특수 목적용 칩이나 모듈 내부에 소량의 점화제나 화학 물질을 내장하여, 탬퍼링 감지 시 칩 패키지를 폭파하거나 회로를 녹여버림으로써 물리적 형상 자체를 없애버리는 기술이다.[6]

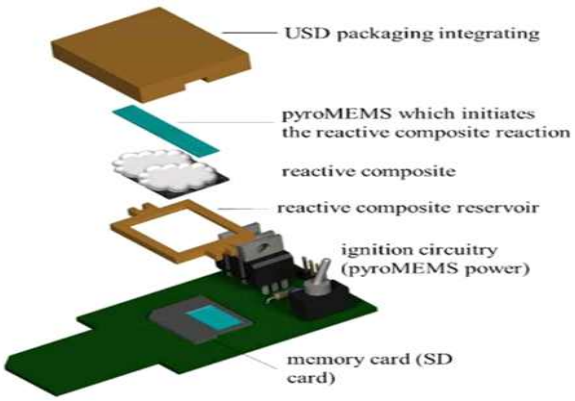

그림 6. 파이로테크닉을 이용한 USD (Ultimate Security Device) [6]

Fig. 6. Ultimate Security Device using pyrotechnics [6]

5. 결론

본 연구는 무기체계 및 정보보호 제품의 핵심 기술 보호를 위한 하드웨어 안티탬퍼 기술과 이를 우회하려는 역공학 분석 기술을 조사하였다. 본 연구를 통해 파악된 국내 안티탬퍼 기술의 가장 큰 문제점은 공용화된 기술 표준과 객관적인 검증 기준의 부재이다. 현재 국내 방산 업체들은 명확한 국가적 기준 없이 사업별 요구사항에 따라 안티탬퍼 기술을 개별적으로 개발한다면, 중복 투자와 기술 파편화가 초래된다. 이는 결과적으로 개발된 기술의 검증도 어렵게 만드는 요인이 된다.

이에 암호모듈 검증 제도(KCMVP)가 보안 강도에 따라 등급을 나누어 관리하듯이, 하드웨어 안티탬퍼 기술에도 보호 대상의 중요도와 위협 수준에 따른 '안티탬퍼 기술 등급' 체계의 도입을 제언한다. 안티탬퍼 기술의 등급 정의 및 표준화는 개발 업체에게는 명확한 개발 목표를, 수요군에게는 객관적인 평가 기준을 제공하게 될 것이다.

Acknowledgment

이 논문은 2022년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-22-051)

This work was supported by the Korea Research Institute for Defense Technology Planning and Advancement(KRIT) - Grant funded by Defense Acquisition Program Administration (DAPA) (KRIT-CT-22-051)

References

[1] “USAF Weapon System Program Protection / Systems Security Engineering Guidebook”, Version 2.0, March, 2020.

[2] Vidaković, Marin, and Davor Vinko. "Hardware-based methods for electronic device protection against invasive and non-invasive attacks." Electronics 12.21, 2023

[3] Asadizanjani, Navid, Mark Tehranipoor, and Domenic Forte. "PCB reverse engineering using nondestructive X-ray tomography and advanced image processing." IEEE Transactions on Components, Packaging and Manufacturing Technology 7.2: 292-299. 2017

[4] Youngjin Joo, et al. “Packaging and Anti-tamper for Critical Technology Protection of Weapon Systems.” Korean Institute of Information Scientists and Engineers, 2024

[5] 송경호, 허아라, and 류연승. "체계공학 기반 안티탬퍼링 프로세스." 한국방위산업학회지 (2021): 77-91.

[6] Sevely, Florent, et al. "Development of a Chip-Level Ultimate Security Device Using Reactive Composites." 2021 IEEE 20th International Conference on Micro and Nanotechnology for Power Generation and Energy Conversion Applications (PowerMEMS). IEEE, 2021.

[7] 주영진, et al. "무기체계 기술보호를 위한 안티탬퍼링 시험평가 방안." 한국방위산업학회지 (2023): 47-58.

[8] 주영진, et al. "무기체계의 핵심기술 보호를 위한 패키징과 안티탬퍼." 한국정보과학회 학술발표논문집 (2024): 41-43.