Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 82-88, 2023

https://doi.org/10.5762/KAIS.2023.24.9.82
ISSN 1975-4701 / eISSN 2288-4688

안티탬퍼링의 동향 및 발전 방향 연구

김민욱
국방기술진흥연구소

A Study of Anti-tampering Trend and Development Direction

Minuk Kim
Korea Research Institute for Defense Technology Planning and Advancement

요 약 2022년 세계 방산시장 연감에 따르면 한국은 세계 25대 무기 수출국 중 8위를 차지하며 방위산업 강국으로 발돋움하고 있다. 우리나라의 무기체계 수출이 증가함에 따라 수출 무기체계 기술 보호 대책의 중요성이 부각 되고 있다. 안티탬퍼라는 용어는 미 국방부에서 처음 사용한 용어로 시스템에 적용된 최첨단 기술을 도난이나 인가되지 않은 용도로 분석되어 변조되는 것을 방지하기 위한 기술로 정의하고 있다. 즉, 안티탬퍼링이란 역공학 및 탬퍼링 공격 시도로부터 자산을 보호하고 기술유출을 방지하기 위한 행위를 의미한다. 본 논문에서는 무기체계 적용 핵심기술을 보호하는 안티탬퍼링 관련 국내·외 제도·정책 및 연구개발 동향의 조사·분석을 수행하고 해당 분야의 발전 방향을 제시한다.

Abstract According to the 2022 Global Defense Market Yearbook, South Korea ranks eighth among the world's 25 largest arms exporters, and South Korea is emerging as a strong country in the defense industry. As exports of weapons systems increase, the importance of technology protection measures is emerging. The term "anti-tamper" was first used by the US Department of Defense. "Anti-tamper" is defined as a technology to prevent cutting-edge technology applied to a system from being stolen or analyzed and tampered with for unauthorized use. In other words, anti-tampering refers to actions to protect assets from reverse engineering and tampering attacks and to prevent technology leakage. We conducted research and analysis of anti-tampering-related systems, policies, and research and development trends to protect core technologies applied to weapon systems. We also present a direction for development in the field of anti-tampering.

Keywords : Anti-Tamper, Anti-Tampering, Tamper Resistance, Weapon System Technology Protection, Core Technology

1. 서론

2022년 세계 방산시장 연감에 따르면 한국은 세계 25대 무기 수출국 중 8위를 차지하여 전년도 통계 대비 1계단 상승하였다[1]. 이러한 추세를 고려할 때 우리나라의 무기체계 수출량은 지속적으로 증가할 것으로 예상된다. 무기체계의 수출량이 증가함에 따라 무기체계에 적용된 우리 핵심기술 유출의 위험성이 증가하는 것은 피할 수 없는 문제이다. 무기체의 핵심기술 유출 대표사례로서는 중국이 F-117 잔해 수집 분석을 통해 자국 스텔스 전투기를 개발한 사례가 있으며[2], 이러한 문제를 예방하기 위해 무기체계에 적용된 핵심기술을 보호하는 기술의 필요성이 증가하고 있다.

본 논문에서는 Fig. 1과 같이 무기체계에 적용된 핵심기술을 보호하는 안티탬퍼링 기술 관련 제도 및 연구개발 동향에 대한 조사분석을 통해 해당 분야의 발전 방향

*Corresponding Author : Minuk Kim(Korea Research Institute for Defense Technology Planning and Advancement)
email: kimminuk@krit.re.kr
Received July 26, 2023 Revised August 28, 2023
Accepted September 1, 2023 Published September 30, 2023

을 제시하고자 한다.

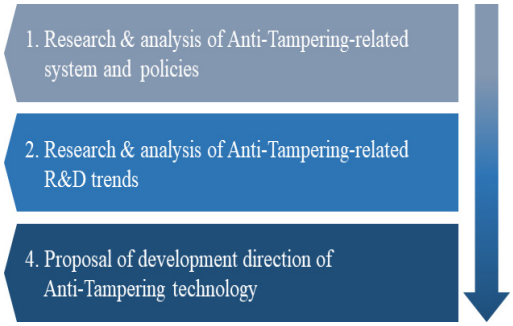

Fig. 1. Research Process Conceptual Diagram

2. 본론

안티탬퍼링에서 탬퍼링이란 단어의 뜻 그대로 시스템의 데이터를 위조하거나 변조하는 행위를 말한다. 안티탬퍼라는 용어는 미 국방부에서 처음 사용한 용어로 시스템에 적용된 최첨단 기술을 도난이나 인가되지 않은 용도로 분석되어 변조되는 것을 방지하기 위한 기술이며, 의도하지 않은 기술 이전 또는 리버스 엔지니어링으로 인한 시스템 변경을 방해하기 위한 시스템 엔지니어링 활동으로 정의하고 있다[3]. 즉, 안티탬퍼링이란 역공학 및 탬퍼링 공격 시도로부터 자산을 보호하고 기술유출을 방지하기 위한 행위를 의미한다.

안티탬퍼링 기술은 앞서 설명한 안티탬퍼링 행위를 수행하기 위해 필요한 기술로 공격자의 탬퍼링 공격에 대비하여 예방 시스템을 갖춰 공격 발생을 방지하고, 공격에 노출되었을 때 신속한 대응을 위한 능동적인 공격 탐지 시스템을 통해 적절한 조치를 수행하여 피해를 최소화하는 목적으로 사용된다.

현재 방위산업 선진국에 해당하는 미국, 영국, 이스라엘에서는 안티탬퍼링 관련 제도 및 정책을 통해 자국의 핵심기술을 보호하기 위해 노력하고 있으며, 국내·외에서 다양한 안티탬퍼링 관련 연구들이 수행되고 있다.

2.1 안티탬퍼링 관련 제도 및 정책

2.1.1 국외 방위산업 선진국의 제도 및 정책

방위산업 선진국에 해당하는 미국, 영국, 이스라엘의 안티탬퍼링 관련 제도 및 정책은 아래 Table 1과 같다.

Table 1. Anti-Tampering Systems and Policies of Advanced Countries in the defense industry

Countries	Systems & Policies
USA	CPI Protection within the DoD
UK	Cyber resilience strategy for defence
	Secure design principles
Israel	Cyber defense methodology for organization

2.1.1.1 미국

미 국방부에는 안티탬퍼 기술에 대해 미 국방부 지침서 DoDI 5200.39 “Critical Program Information(CPI) Protection Within the Department of Defense”에 기반한 종합적인 정책이 존재한다. 이 정책은 미 국방부 프로그램 매니저가 각 수요 프로그램에 대한 정책 수립 및 CPI를 식별하고, 무단 접근, 수정 또는 악용을 방지하기 위한 안티탬퍼 조치를 포함한 보호 계획을 개발하도록 요구하고 있다. 이 정책은 안티탬퍼 요구사항을 설계, 개발, 테스트 및 유지 관리의 각 단계에서 적용하도록 지시하고 있으며 미 국방부 내 모든 조직에 적용된다.

해당 정책을 지원하기 위해 미 국방부는 ATEA (Ati-Tamper Executive Agent)를 설립하여 모든 미 국방부 프로그램에 대한 안티탬퍼링 조치, 지침·자원 관리 및 감독을 수행하고 있다.

2.1.1.2 영국

영국 국방부는 자국의 사이버 강국으로서의 권위를 강화하기 위한 전략인 “Cyber resilience strategy for defence”를 발표하였으며, 해당 전략의 목표를 달성하기 위한 7가지 전략적 우선순위를 아래 Fig. 2와 같이 발표하였다.

해당 전략은 안티탬퍼링에 대한 명시적인 정책을 포함하고 있지는 않지만 7가지 전략적 우선순위 중 “Secure by Design"에 국방 디지털 환경에 국제표준 및 NCSC(National Cyber Security Centre, 영국 국립사이버보안센터)의 보안 설계 핵심 원칙 적용하는 등 포괄적인 보안 설계 프로세스를 포함하고 있다.

NCSC의 5가지 보안 설계 원칙은 아래 Fig. 3과 같다. NCSC의 5가지 보안 설계 원칙 중 "2. Make Compromise difficult"는 보안을 염두에 둔 설계를 통해 공격자에 의한 데이터 및 시스템 손상을 어렵게 만드는 개념을 포함하고 있어 안티탬퍼링과의 직접적인 관련성이 존재한다.

Fig. 2. "Cyber resilience strategy for defence" 7 Strategic Priorities[4]

Fig. 3. Cyber Security design principles[5]

2.1.1.3 이스라엘

이스라엘 국가사이버국(Israel National Cyber Directorate)에서는 이스라엘 내 모든 조직에 대한 권장사항으로 보안 강화를 방법론을 개발하였다. 해당 방법론은 프로그램 개발 프로세스에 디지털 서명, 암호화 같은 변조 방지 메커니즘을 포함하고, 데이터 탈취, 변조, 삭제를 예방하기 위한 조치를 의무적으로 수행하도록 하는 등 안티탬퍼링 관련 항목을 포함하고 있다[6].

2.1.2 국내 안티탬퍼링 관련 제도 및 정책

국내에서는 방위사업청 행정규칙인 "방위산업기술 보호지침(방위사업청 훈령 제797호, '23. 5.16.)"에서 무기체계 연구개발 사업 및 기술연구개발사업의 기술보호에 대한 세부사항과 수출 및 국내이전 시 기술보호에 대한 세부사항을 규정하고 있다.

특히, 해당 행정규칙 "제38조(수출 및 국내이전 시 방위산업기술 보호체계 구축·운영)의 ④항" 및 "별표 11. 수출 시 방위산업기술 보호대책"에서는 수출 무기체계에 대한 안티탬퍼링 등 기술보호기법의 적용 계획을 필수로 제시하도록 하고 있다.

2.2 안티탬퍼링 기술

안티탬퍼링 기술은 중요 자산과 데이터를 안전하게 보호하기 위해 하드웨어와 소프트웨어에 모두 적용이 필요하지만, 하드웨어에 적용 가능한 안티탬퍼링 기술은 신뢰 실행 환경(Trusted execution environment, TEE)을 지원하는 칩을 사용하거나 부채널 공격에 강인한 칩을 사용하는 등 칩 레벨에서 제공하는 기능을 제외하면 봉인지 부착, 다양한 형상의 나사를 사용하는 등 기초적인 방법과 센서를 활용하여 조립체 무단 개봉이 감지되면 핵심기술이 저장되어있는 저장장치를 초기화하거나, 폭파하는 등 물리적 방법을 활용하여 보호 대상 장비의 기능을 무력화하는 등의 방법으로 한정되어있다.

소프트웨어 안티탬퍼링은 소프트웨어의 역공학 분석으로 인한 위변조를 막는 기술을 말한다. 기술의 목적에 따라서 억지, 예방, 탐지 대응으로 구분할 수 있으며 해당 목적을 달성하기 위한 세부기술들이 존재한다.

먼저 억지 기술은 해당 기술 자체로 위변조를 억지하는 방법이다. 해시, 체크섬 등을 통해 무결성을 검증하는 기술의 적용을 통해 공격 시도 자체를 억지하는 방법으로 대부분의 소프트웨어 안티탬퍼링 기술들이 이에 해당된다고 할 수 있다. 예방 기술은 위변조를 예방하기 위한 기술로 리버싱을 어렵게 만드는 암호화, 난독화 등을 통해 소프트웨어 기반 데이터를 숨기거나 복잡도를 증가시키는 등의 행위를 통해 유효 데이터의 획득을 어렵게 만드는 방법이다. 탐지 기술은 위변조 시도가 발생했을 시 이를 탐지하기 위한 기술을 말하며 인증, 접근제어, 무결성 탐지 기술이 이해 해당된다. 마지막으로 대응 기술은 위변조 시도가 탐지되었을 때 취할 수 있는 행동을 뜻하며 리포팅, 저장장치 리셋 등이 이에 속한다.

앞서 살펴본 각국의 안티탬퍼링 관련 제도 및 정책과 소프트웨어 안티탬퍼링 기술들에서 알 수 있듯이 소프트웨어에 적용 가능한 안티탬퍼링 기술은 완전히 새로운 기술이라기보다는 기존의 사이버보안에 활용되는 정보보호 분야 기술의 활용이라 말할 수 있다.

2.3 안티탬퍼링 연구 동향

2.3.1 국외 연구동향

국외에서는 무기체계 안티탬퍼링 기술로 활용될 수 있는 다양한 정보보호 분야 기술의 연구가 진행되고 있다. 최근 3년간 진행된 정보보호 분야의 연구 중 안티탬퍼링 기술로 활용이 가능할 것으로 판단되는 대표적인 연구사례들은 아래와 같다.

"HRPDF" 연구에서는 PLC 호환 가능한 소프트웨어 기반 기법을 통해 능동적인 보안 프레임워크를 제시하였다. PLC 소프트웨어는 펌웨어 변조 공격, 제어 로직 변조 공격, 메모리 공격이 발생할 수 있는데, PLC 보안 프레임워크인 HRPDF는 ASLR 기법으로 코드, 환경설정, 객체 세그먼트 같은 실행 중에 메모리에 존재하는 데이터를 보호하고, 리버싱 분석을 어렵게 하기 위한 난독화 기법을 적용하여 컴파일 시 쓸모없는 명령어를 삽입하고, 프로시저콜의 주소를 숨기기 위해 점프 테이블을 적용하여 제어 로직을 보호하였다.

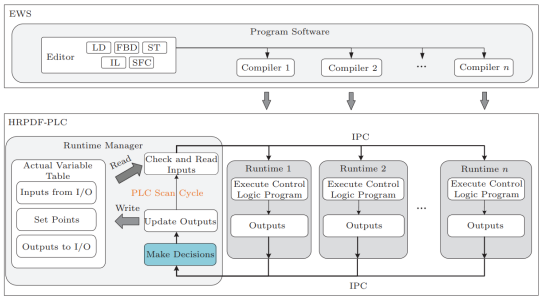

Fig. 4. HRPDF Architecture[7]

"Software Protection Using Dynamic PUFs" 연구에서는 동적 PUFs(Physical Unclonable Functions)를 사용하여 소프트웨어 보호를 강화하는 방법에 대해 제안하였다. PUF는 하드웨어 칩에서 고유한 ID를 생성하는 기술로, 복제 불가능하고 위조 불가능한 보안 기능을 제공한다. 제안한 HESP(Hardware Entangled Software Protection) 프레임워크는 동적 PUF로 소프트웨어를 보호하기 위해 코드 실행 중에 PUF 값을 생성한다.

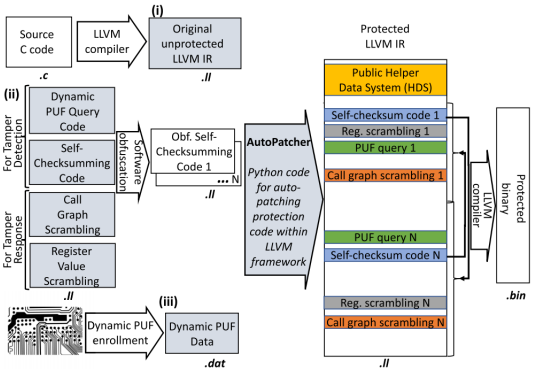

Fig. 5. HESP Framework[8]

"Khaos: The Impact of Inter-procedural Code Obfuscation on Binary Diffing Techniques" 연구에서는 바이너리 디핑을 통한 취약점 분석을 방지하기 위해 코드를 함수 사이로 이동시키는 새로운 코드 난독화 메커니즘인 Khaos를 제안하였다.

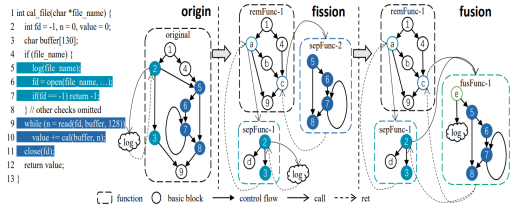

Fig. 6. Example of Khaos Obfuscation Function [9]

"Generating Effective Software Obfuscation Sequences With Reinforcement Learning" 연구에서는 코드 암호화 및 코드 분할과 같은 기존의 난독화 기법은 의도적인 공격자가 쉽게 우회할 수 있다고 주장하였고, 머신러닝 방식을 사용하여 효율성이 최적화된 난독화 시퀀스를 생성할 것을 제안하였다. 제안된 접근 방식은 머신러닝의 하위 분야인 강화학습을 사용하여 신경망을 훈련시켜 난독화 시퀀스를 생성한다[10].

2.3.2 국내 연구동향

국내에서도 안티탬퍼링 기술로 적용할 수 있는 다양한 정보보호 분야의 연구개발이 국방과제의 형태로 수행되고 있으며, 방위사업청이 2023년 발간한 '23-'37 국방기술기획서 일반본에 의하면 아래 Table 2와 같이 3개(세부 과제 기준 7개)의 안티탬퍼링 분야 국방과제 연구개발이 진행 중인 것을 확인할 수 있다.

Table 2. Defense R&D Status of Anti-Tampering Technology

Category	Programs	
Core SW	Weapon System SW Platform Anti-Tampering Technology	
Applied Research	Weapon System Anti-Tampering Application Technology	
Weapon System Package Type	Weapon System Technology Protection Technique (Anti-Tampering)	Development of Packaging Ant-Tampering and System Intergration Technology
		Development of Board/Chip Anti-Tampering Technology
		Development of Code Anti-Tampering Technology
		Development of SW Anti-Tampering Technology
		Development of Anti-Tampering Test/Verification Technology

국방과학연구소 주관으로 연구개발을 진행 중인 “무기체계 소프트웨어 플랫폼 안티탬퍼링 기술” 과제는 무기체계 소프트웨어 정보의 탈취를 방지하기 위하여 HW/SW의 탈취 및 복제를 방지하는 안티탬퍼링 기술을 개발하여 무기체계에 공통적으로 사용 가능한 무기체계 소프트웨어 플랫폼 안티탬퍼링 기술을 개발하는 응용연구 단계의 핵심SW 과제로 무기체계 플랫폼 템퍼링 감지 기술 연구, 무기체계 플랫폼 템퍼링 차단 Guard 기술 연구, 안티템퍼링 테스트베드 구축/시험 및 코드 안티템퍼링 기법 연구를 주요 연구항목으로 포함하고 있다[11].

국방과학연구소 주관으로 연구개발을 진행 중인 “무기체계 안티탬퍼링 적용기술” 과제는 파괴적/비파괴적 탬퍼링 대응을 위한 안티탬퍼링 기술과 무기체계 기능/성능 영향을 최소화하는 안티탬퍼링 통합 기술을 개발하는 응용연구 단계의 과제로 탬퍼링 차폐 기술, 부채널 분석 방지 기술, 임베디드 시스템 TEE(Trusted Execution Environment) 적용 기술을 주요 연구항목으로 포함하고 있다[12].

산학연 주관으로 연구개발을 진행 중인 “무기체계 기술보호기법(Anti-Tampering)” 과제는 아래 Fig. 7과 같이 5개의 응용연구 단계 과제로 구성되어있는 무기체계 패키지형 프로그램으로 무기체계를 대상으로 하는 비인가자의 역공학 공격에 대한 대응책 및 의도하지 않은 기술의 이전 또는 시스템 변경을 방지하기 위해 단계적 심층 방어 개념의 안티탬퍼링 기술을 개발하는 프로그램이다[13].

종합과제인 “패키징 안티탬퍼링 및 체계 통합 기술 개발”은 패키징 안티탬퍼링 기술을 개발하고 보드/칩 안티탬퍼링 기술, 코드 안티탬퍼링 기술, SW 안티탬퍼링 기술 및 안티탬퍼링 시험검증 기술을 무기체계와 유사한 형태의 시범체계에 적용하여 안티탬퍼링 기능/성능 검증

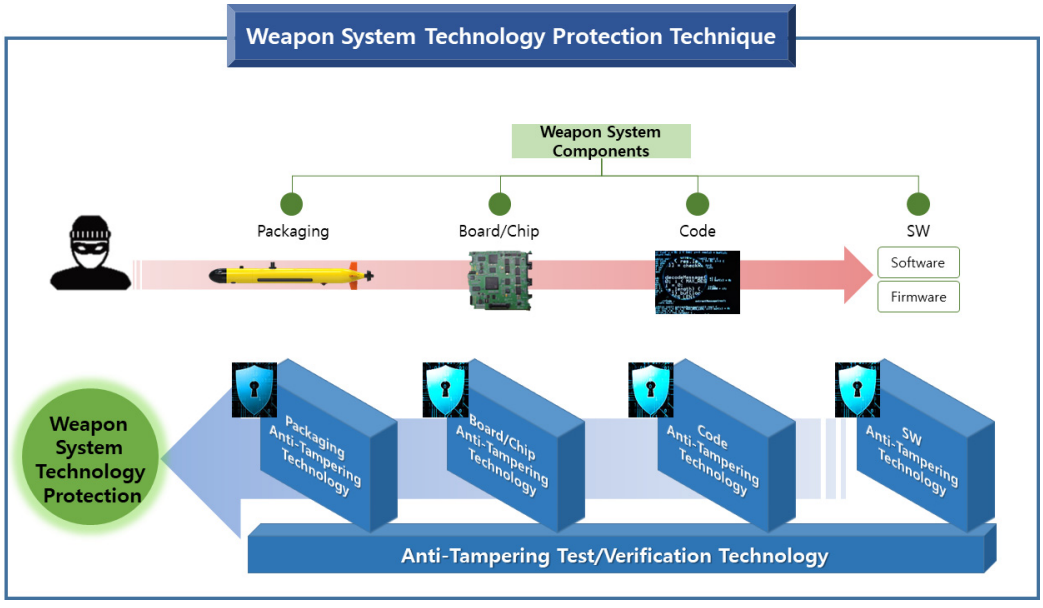

Fig. 7. "Weapon System Technology Protection Technique (Anti-Tampering)" Program Technology Development Concept Map

및 안티탬퍼링 기술 적용에 따른 체계 영향성 검증을 목표로 하는 과제로 능동형 접근 방지 기술, 패키징 접근 감지 및 차단 기술, 시범체계 구축을 주요 연구항목으로 포함하고 있다.

“보드/칩 안티탬퍼링 기술 개발”은 무기체계 운용 환경에 알맞은 탬퍼링 위협 차단 HW 보안 모듈 기술, 기술 보호 대상 무기체계와 연동하여 탬퍼링 위협을 차단하는 플랫폼 기술, 탬퍼링 위협을 차단하는 무기체계 응용 기술을 개발하여 무기체계용 보드/칩 수준에서 안티탬퍼링을 제공하는 무기체계용 보드/칩 안티탬퍼링 기술을 개발하는 과제로 탬퍼링 차단 HW 보안 모듈 기술, 탬퍼링 차단 플랫폼 기술, 탬퍼링 차단 무기체계 응용 기술을 주요 연구항목으로 포함하고 있다.

“코드 안티탬퍼링 기술 개발”은 대상 코드에 대한 역공학 공격에 대응하기 위한 코드 역공학 방지 기술, 암호화 코드가 공개되어 화이트박스 공격이 가능한 상황에서도 비밀키가 노출되지 않도록 체계적인 키 관리를 통해 안전한 암호화 알고리즘을 제공하는 화이트박스 공격 대응 암호화 기술, 물리 채널 취약점을 제거하는 고보증 물리채널 방어기술을 주요 연구항목으로 포함하고 있다.

“SW 안티탬퍼링 기술 개발”은 무기체계 소프트웨어 부팅 및 실행 시 사전 검증을 통해 무기체계 소프트웨어 변조를 확인하는 무기체계 변조 방지 기술, 체계-부체계 간 통신 또는 유지보수용으로 사용되는 무기체계 인터페이스의 보안 취약점을 목표로 하는 탬퍼링 공격을 차단하기 위한 무기체계 인터페이스 안티탬퍼링 기술, 무기체계를 구성하는 구성품의 이상 유무 또는 무기체계 소프트웨어를 구성하고 있는 파일 감시를 통해 실행 중 침입을 탐지하고 침입에 대한 차단 등의 대응을 수행하는 능동형 탬퍼링 위협 대응 기술 개발을 주요 연구항목으로 포함하고 있다.

“안티탬퍼링 시험/검증 기술 개발”은 각 단위과제에서 연구개발을 수행하는 패키징 안티탬퍼링, 보드/칩 안티탬퍼링, 코드 안티탬퍼링, SW 안티탬퍼링 기술에 대해 일반적으로 적용 가능한 시험/검증 방법 및 기술을 확보하고 이를 각 세부과제별 단위 시험/검증에 적용하는 것을 연구개발 목표로 하고 있다.

앞서 살펴본 연구개발 사례들에서 알 수 있듯이 국내에서는 안티탬퍼링의 기반기술로 활용할 수 있는 정보보호 기술뿐만 아니라 무기체계에 직접 적용이 가능한 실효성 있는 안티탬퍼링 기술의 연구개발이 국방 연구개발 사업의 형태로 수행되고 있다.

3. 결론

본 논문에서는 국내·외 안티탬퍼링 관련 제도 및 정책과 안티탬퍼링 관련 기술의 연구개발동향을 살펴보았다.

우리나라의 무기체계 수출량은 지속적으로 증가할 것으로 예상되며, 무기체계의 수출량이 증가할수록 우리 무기체계에 적용된 핵심기술을 대상으로 한 탬퍼링 및 역공학 공격 또한 점차 증가하는 것은 피할 수 없는 문제이다. 이러한 공격에 따른 핵심기술 유출 문제를 예방하기 위해 무기체계에 핵심기술을 보호하기 위한 안티탬퍼링 기술을 적용하는 것은 필수적이며, 안티탬퍼링 기술은 기술을 보호하기 위한 기술이라는 점에서 관련 제도 및 정책에서 분리될 수 없다는 특수성이 존재한다.

앞서 국외 사례에서 살펴보았듯이 미국, 영국, 이스라엘 등 방위산업 선진국에서는 안티탬퍼링 관련 제도·정책 운영을 통해 자국의 기술을 보호하고 있으며, 특히 미국에서는 안티탬퍼링을 위한 전담 조직인 ATEA를 운영하고 있다.

국외뿐만 아니라 국내에서도 무기체계의 기술보호를 위한 안티탬퍼링기술 적용의 중요성을 인식하여 관련 규정 개정을 통해 수출 무기체계에 대한 기술보호기법 적용을 명시화하고 있으며, 국방과학연구소 및 산학연을 중심으로 하는 안티탬퍼링 기술의 연구개발을 수행 등 다양한 노력이 이루어지고 있다.

하지만, 현재 국내에서 연구개발을 수행 중인 국방기술 연구개발 과제는 모두 실험실 환경에서 기술의 타당성과 실용성을 입증하는 응용연구 단계의 과제이다. 실효성을 가지는 연구개발이 되기 위해서는 시제품을 제작을 통해 무기체계 적용 가능성과 미래무기체계에 대한 응용 가능성을 입증하는 시험개발 단계 과제의 추가적인 연구개발 수행이 필요할 것으로 예상된다.

또한, 현재 국내에는 안티탬퍼링 전반에 대한 조치, 지침 관리 및 감독을 전담하는 미국의 ATEA와 같은 안티탬퍼링 전담 조직이 부재한 상황이다.

따라서, 국내 안티탬퍼링 분야의 발전을 위해서는 연구개발뿐만 아니라 제도·정책 전반에 대한 추가적인 노력이 필요하다.

References

[1] Korea Research Institute for Defense Technology Planning and Advancement, Global Defense Market

Yearbook 2022, pp.44-48, Dec. 2022.

[2] Defense Acquisition Program Administration, Technology Protection Technique Development Status and Policy Promotion Direction
https://www.dapa-magazine.kr/page/vol109/view.php?volNum=vol109&seq=5
(accessed JUL. 22. 2023)

[3] Department of Defense, Department of Defense DIRECTIVE(SUBJECT : Anti-Tamper(AT), NUMBER : 5200.47E), USA, p.7

[4] British Ministry of defense, Cyber Resilience Strategy for Defence, p.6, Apr. 2022.

[5] National Cyber Security Centre, Secure Design Principles
https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles
(accessed JUL. 22. 2023)

[6] Israel-National Cyber Directorate, Cyber Defense Methodology for an Organization, pp.12-32

[7] Ke Liu, Jing-Yi Wang, Qiang Wei, Zhen-Yong Zhang, Jun Sun, Rong-Kuan Ma, Rui-Long Deng. "HRPDF: A Software-Based Heterogeneous Redundant Proactive Defense Framework for Programmable Logic Controller", Journal of Computer Science and Technology, 2021, 36(6): 1307-1324
DOI: https://doi.org/10.1007/s11390-021-1647-7

[8] Wenjie Xiong, André Schaller, Stefan Katzenbeisser, Jakub Szefer, "Software Protection Using Dynamic PUFs", IEEE Transactions on Information Forensics and Security, VOL. 15, 2020
DOI: https://doi.org/10.1109/TIFS.2019.2955788

[9] Peihua Zhang, Chenggang Wu, Mingfan Peng, Kai Zeng, Ding Yu, Yuanming Lai, Yan Kang, Wei Wang, and Zhe Wang. "Khaos: The Impact of Inter-procedural Code Obfuscation on Binary Diffing Techniques", In Proceedings of the 21st ACM/IEEE International Symposium on Code Generation and Optimization (CGO '23), Montréal, QC, Canada. ACM, New York, NY, USA, February 25–March 1, 2023
DOI: https://doi.org/10.1145/3579990.3580007

[10] Huaijin Wang, Shuai Wang, Dongpeng Xu, Xiangyu Zhang, Xiao Liu, "Generating Effective Software Obfuscation Sequences With Reinforcement Learning", IEEE Transactions on Dependable and Secure Computing, VOL. 19, NO. 3, May/June 2022.
DOI: https://doi.org/10.1109/TDSC.2020.3041655

[11] Defense Acquisition Program Administration,, '23-'37 General Copy of Defense Technology Plannig, p,260, May. 2023

[12] Defense Acquisition Program Administration,, '23-'37 General Copy of Defense Technology Plannig, p,178, May. 2023

[13] Korea Research Institute for Defense Technology Planning and Advancement, Request for Proposal of "Weapon System Technology Protection Technique (Anti-Tampering)"
https://dtims.krit.re.kr/vps/OINF_CtPrjNotiList.do
(accessed JUL. 22. 2023)

김 민 욱(Minuk Kim) [정회원]

- 2016년 2월 : 경상국립대학교 항공우주 및 소프트웨어공학부 (학사)
- 2016년 1월 ~ 2020년 7월 : 퍼스텍(주) 선임연구원
- 2020년 9월 ~ 2020년 12월 : 국방기술품질원 연구원
- 2021년 1월 ~ 현재 : 국방기술진흥연구소 연구원

〈관심분야〉
국방기술기획, 정보통신