Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 4 pp. 470-478, 2019

https://doi.org/10.5762/KAIS.2019.20.4.470
ISSN 1975-4701 / eISSN 2288-4688

무기 시스템의 기술 보호를 위한 CMVP 표준 기반의 Anti-Tamper 시스템 요구사항 도출

이민우, 이재천*
아주대학교 시스템공학과

Derivation of Anti-Tamper System Requirements Based on CMVP Standard for Technology Protection of Weapon Systems

Min-Woo Lee, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 국내 방산분야의 기술적 성장과 수출 증대가 괄목함에 따라, 국가안보적 위협을 방지하기 위한 방위산업 분야 기술보호의 중요성이 강조되고 있으므로 기술보호 제도의 확립 및 수행이 필요하다. 특히 무기 시스템으로부터 중요기술을 불법으로 탈취하는 Tampering 시도에 대응하기 위한 Anti-Tampering 기법의 도입 필요성이 대두되고 있으나, 아직까지는 관련제도가 갖춰지지 않았고 기술자료 유출 예방 위주 수준의 활동이 이루어지고 있다. 선행연구로서 특정 기술 보호기법에 대한 기술적 연구와 동향 분석, 일부 절차를 적용한 Anti-Tampering 적용방안 등이 발표되었으며, 최근에는 위험관리 절차를 기반으로 보호대상 기술을 선정하는 방법이 연구되었다. 하지만 기존 연구들은 무기 시스템의 Life-cycle 차원에서 획득 프로세스와 연계하기에 용이하지 않거나, 실제로 개발 및 평가에서 활용하기는 어려운 것으로 판단된다. 이러한 문제를 해결하는 한 방법으로, 본 논문에서는 Anti-Tampering 적용이 결정된 무기 시스템의 개발에 직접적으로 활용될 수 있는 Anti-Tampering 요구사항의 도출에 대하여 연구하였다. 구체적으로, 암호 모듈의 개발 및 검증에 적용되는 CMVP 표준인 ISO/IEC 19790을 기반으로 무기 시스템 개발에 필요한 요구사항 항목들을 도출하였으며, 기술검토회의 및 시험평가 등에서의 활용방안을 제시하였다. 귀납적 추론 및 비교평가를 통해 연구결과의 유용성을 확인하였다. 본 연구의 결과들을 활용하면, 국내개발 무기 시스템의 본격적인 기술보호 활동 수행에 도움이 될 것으로 기대된다.

Abstract As the growth of the domestic defense industry is remarkable regarding technology level and export size, technology protection is necessary. Particularly, there is a need to apply anti-tamper measures to prevent critical technologies from illegally being taken out of weapon systems. However, there is no security protection strategy and system built yet in ROK. Precedent studies discussed the trend analysis and technical research for specific protective techniques, and the application of anti-tamper using limited procedures was provided. Recently, methods of how to select the technology for protection were studied based on risk management. Nonetheless, these studies cannot be associated with the acquisition process for the whole life-cycle, having difficulty with actual development and evaluation of the weapon systems. The objective of our study is to derive the system requirements of the weapon system for which anti-tamper measures have been determined to apply. Specifically, requirements items suitable for the development of anti-tamper weapon systems were derived based on ISO/IEC 19790, the CMVP standard for the development and verification of cryptographic modules. Also, its utilization in technical reviews and test & evaluations was presented. The usefulness of the research results was confirmed through inductive inference and comparative evaluation. The result can be expected to play a role in initiating extensive activities needed for technology protection of the weapon systems.

Keywords : Anti-Tamper, Technology Protection, Weapon Systems R&D, Systems Engineering, Requirement Engineering

*Corresponding Author : Jae-Chon Lee(Ajou Univ.)
Tel: +82-31-219-3941 email: jaelee@ajou.ac.kr
Received January 11, 2019 Revised February 7, 2019
Accepted April 5, 2019 Published April 30, 2019

1. 서 론

한국의 무기 시스템 개발역사도 어느덧 48년이 지났고, 초기의 보잘 것 없던 모조품 생산 능력이 이제는 국가가 앞장서 지켜야 하는 중요한 자산이 되었다. 방위산업 관련기술의 유출은 경제적 손실 뿐만 아니라 국가안보에 직접적인 영향을 미치기 때문에 그 중요성이 남다르다 할 수 있으며 최근 다양한 기술침해 시도가 지속되고 있기에 대비가 필요하다[1]. 방산분야 기술보호는 기술자료 뿐만 아니라 해당 기술을 바탕으로 생산·배치된 무기 시스템을 대상으로도 이루어져야 하며 이를 위해 Anti-Tamper라는 SE 활동이 필요하다[2,8].

방위사업청 국방기술보호국에서 기술보호 관련 정책을 추진하고 있으나 Anti-Tamper 관련제도는 아직 미비하며, 선행연구의 경우 특정 보호기법의 발전을 위한 기술적 연구[3-4], 관련동향 분석 및 일부 절차만을 선택적으로 접목하는 내용만을 다루고 있다[5-7]. 그러므로 국내개발 무기 시스템에 Anti-Tamper를 적용하여 기술을 효과적으로 보호하는 것은 아직은 다소 어렵다고 판단된다.

이러한 인식에 따라 위험관리(Risk-Management) 절차를 기반으로 Anti-Tamper 적용대상 기술 선정방법을 도출한 바 있으나[8], 선정된 기술을 보호하기 위한 구체적인 요구사항은 제시되지 않았다.

본 논문에서는 보다 구체적으로 Anti-Tamper를 적용하기 위해 무기 시스템 개발 요구사항을 도출하였다. 이를 위해 정보보호체계에 사용되는 암호모듈의 검증을 위한 CMVP(Cryptographic Module Validation Program) 관련 국제표준을 적용하였다. CMVP는 보안등급별로 개발 및 검증 요구사항이 차등화되어 있으며[9-10] 이를 바탕으로 시스템 개발 수행 간 손쉽게 활용이 가능한 무기 시스템 개발 요구사항을 도출할 수 있었다.

이어지는 2장에서 Anti-Tamper 적용의 필요성과 현실태, 선행연구 동향 및 연구목표를 제시하였다. 3장에서는 CMVP 표준들을 적용하여 Anti-Tamper 개발 요구사항들을 도출하였고 4장에서는 도출된 요구사항 활용에 따른 무기 시스템 기술보호 향상 여부를 분석하여 연구결과가 타당함을 제시했다. 마지막 5장에서는 연구결과를 정리하였다.

2. 문제의 정의

2.1 Anti-Tamper 적용의 필요성

국방부·방사청 등의 정부기관, 합참·소요군, 국과연·기품원 등의 출연기관뿐만 아니라 방산관련기업에 이르기까지 적성국 및 제3국으로부터 다양한 방법 및 경로로 기술자료를 탈취하기 위한 시도가 지속되고 있다[11]. 이에 따라 방위사업청 국방기술보호국(구. 방산기술통제관)에서는 「방위산업기술보호법」을 제정하였으며, 기술보호 관련 기반구축을 위한 다방면의 활동을 수행하고 있다. 방위산업기술보호 제도는 국방과학기술 중 보호대상으로 고시된 "방위산업기술"을 보유한 "대상기관"이 효율적으로 기술보호체계를 구축·운영하도록 지원하는 것이라 할 수 있다[1].

그러나 Fig. 1 과 같이 총수명주기적 관점에서 기술탈취 유형을 살펴보면, 기술보호체계 구축 및 운영을 통해 내·외부로부터의 군사기밀 및 기술자료의 유출 위험은 감쇄시킬 수 있겠지만 무기 시스템 양산 이후 Hijacking, Tampering 등의 경우 현재로서는 뚜렷한 대응책이 없다고 판단된다.

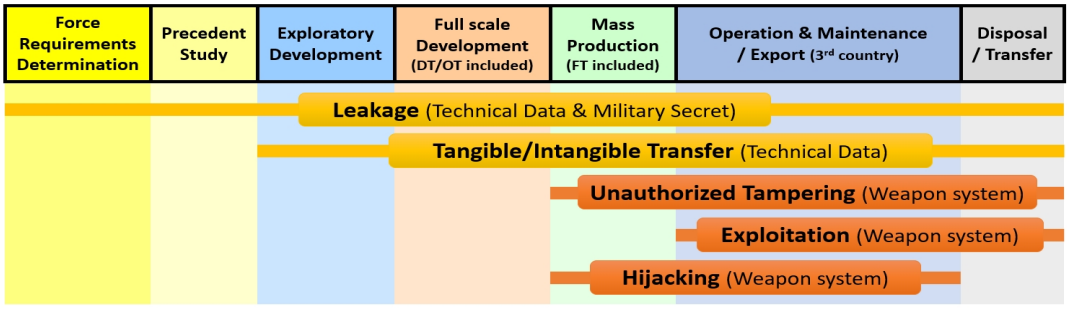

Fig. 1. Tech. leakage cases in 'Total life-cycle' viewpoint

우리가 개발한 무기 시스템이 적성국 군 관계자 및 해커, 방산 경쟁국 개발자 등에 의해 Hijacking 또는 Tampering 되는 경우 역설계 등에 의해 무기 시스템에 적용된 핵심기술이 유출되어 단시간 내 동등 이상의 대응무기(Countermeasure Weapons)가 등장하거나, 우리 군 병사를 공격하는 등의 피해가 발생할 수 있으므로 반드시 이에 대한 방어수단을 마련해야 한다[2,8].

미 국방성의 “DoDI 5200.39”에 따르면, 미국은 무기 시스템 개발에 필요한 기술정보, 군사기밀 등“사업 중요정보”(CPI, Critical Program Information) 유출 예방을 위해 무기 시스템 획득사업 수행 시 PPP(Program Protection Plan)라는 계획을 수립하여 다양한 활동을 수행하고 있다[12]. 특히 그 중에서 무기 시스템의 CPI를 보호하기 위한 활동을 Anti-Tamper 라 하며, “DoDD 5200.47E”에 따르면 이는 “미 국방 시스템에 담긴 CPI 이용을 방지하거나 지연시키기 위한 Systems Engineering 활동”으로 정의된다[2]. 지연시킨다는 의미는 무기 시스템에 대한 Tampering 등의 접근을 계속 완벽히 방어할 수 없으므로 미국이 훨씬 발전된 기술을 보유하게 되는 시점까지 기술유출을 방지하겠다는 것이다.

미국은 무기 시스템의 개발 프로세스에 4가지의 Evaluation Points를 두고 있으며 각각의 평가 시점에서 Anti-Tamper 개념, 실행계획, 설계검증 · 확인결과 등을 검토하고 있다[13]. Anti-Tamper 기술적 기법들은 아래의 4가지 보호기법 유형으로 분류할 수 있는 것으로 알려져 있다[8].

- Tamper Deterrence(억제) : 봉인지, 라벨 등으로 불필요한 접근이 금지되어 있음을 경고한다. 수출용 무기 시스템의 경우, 계약조항과 정비교범에도 해당 내용을 포함하여 법적 책임이 있음을 강조할 수 있다.
- Tamper Detection(감지) : 비인가 접근에 대해 기록하여 차후 확인 시 책임을 묻도록 하거나 방지 또는 반응기법의 트리거로서 활용된다.
- Tamper Resistance(방지) : 핵심기술이 포함된 Components 및 Parts에 대한 접근을 방해하는 기법으로서, 특수공구 또는 Crypto Key 등을 통해서만 접근이 가능하도록 하거나 회로도의 코팅, 데이터 암호화 등의 기술적 조치이다.
- Tamper Response(반응) : 방지기법의 적용에도 불구하고 비인가자가 이를 파훼하여 핵심기술 도달이 임박한 경우 회로기판 또는 프로그램 등이 스스로 파괴/삭제되어 핵심기술 탈취를 실패하게 만드는 조치이다. 반응기법 발동 시 무기 시스템은 정상작동하지 않게 된다.

2.2 관련 선행연구

Anti-Tamper에 관련된 미 국방성의 자료는 가장 기본적인 지침들을 제외하면 대부분 비공개되어 있으며, 우리나라는 아직 제도가 존재하지 않는다. 선행연구의 경우 S/W 위주의 더욱 강한 보호기법 연구[3-4], 기술동향 분석[5-6], 개발 프로세스와는 무관하게 적용한 사례연구[6-7] 등이 있었다.

따라서 국내개발 무기 시스템에 Anti-Tamper를 적용하기 위한 연구가 필요하였으며, 이에 따라 미 회계감사국(GAO) 감사결과[13-14] 등을 고려하여 무기 시스템의 요소기술들 중에서 Anti-Tamper를 적용하여 보호할 기술의 선정방법과 보호기법의 순차적 Functional flow, 적용수준의 결정방법 등이 연구되었으나[8] 보호대상 기술이 선정된 이후의 구체적인 수행내용은 제시되지 않았다.

한편, 미국 국방안보협력국(DSCA)에서 발행한 “DSCA 00-07” 에서 Fig. 2 와 같은 Anti-Tamper의 구현 프로세스를 확인할 수 있는데[15], 이는 다소 추상적인 활동을 나타내고 있으므로 정부 관계자의 활동에는 일부 도움이 되지만 시스템 개발자가 활용하기는 다소 어려운 것으로 판단된다.

2.3 연구목표 및 범위

무기 시스템 기술보호를 위한 Anti-Tamper 관련 선행연구를 분석한 결과를 바탕으로 아래와 같이 본 논문의 연구목표를 설정하였다.

- 무기 시스템 개발에서 효과적인 Anti-Tamper 기법 적용을 위해 개발자들이 실제로 활용할 수 있는 시스템 요구사항을 도출
- 무기 시스템의 수명주기 관점에서 기술보호를 위해 Anti-Tamper 관련 시험평가 및 운영유지 단계에서 활용할 수 있는 요구사항을 도출

이를 통해 보다 효율적으로 무기 시스템에 Anti-Tamper를 적용할 수 있을 것으로 판단한다.

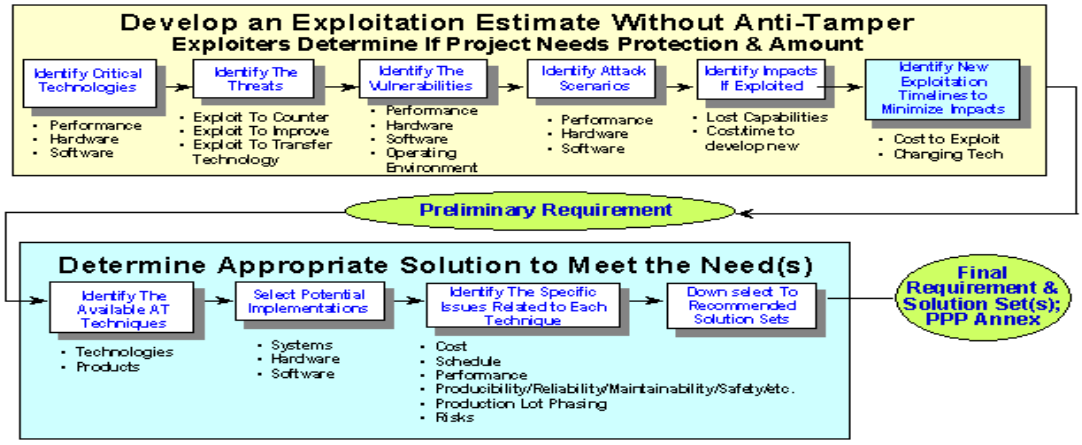

Fig. 2. Anti-Tamper Implementation Decision Process[15]

3. 무기 시스템 기술보호를 위한 Anti-Tamper 요구사항 도출

3.1 Anti-Tamper 요구사항에 대한 CMVP 표준의 적용 필요성 도출

Anti-Tamper 적용을 위한 시스템 개발 요구사항 도출에는 암호 모듈의 개발 및 검증을 위한 CMVP표준을 적용하는 것이 타당한 것으로 판단하였다.

이러한 판단은 암호모듈 및 무기 시스템 간의 공통점에 그 기반을 둔다. 암호모듈은 다양한 정보 시스템이 내부정보를 보호할 수 있도록 시스템의 '보안성' 구현을 위해 사용되는 것이며 H/W 또는 S/W(Firmware 등 포함) 로 이루어진다[16-17]. 특히 H/W 암호모듈의 경우 아래와 같이 무기 시스템과 유사성이 존재한다.

- 중요정보들이 유통되는 네트워크에 직·간접적으로 접속하거나 정보를 직접 전송한다.
  (예 : 금융기관 전산망·軍 지휘통신망 접속, 피아식별 신호 전송 등)
- 비인가자가 악의적으로 접근할 경우 복제 및 역설계 등을 통해 심각한 결과로 이어진다.
  (예 : 개인정보 대량유출, 금융피해, 군사기밀 및 핵심기술 유출, 무기 시스템 조작 등)
- 특성을 고려한 적절한 보호수준이 필요하다.
  (과도한 보호수준에 따른 개발일정 지연 및 비용 증가 등 악영향이 예상되며 반대의 경우 중요한 정보의 적절한 보호 제한)

이어지는 3.2절에서 Anti-Tamper 요구사항 도출 시 적용될 CMVP 표준에 대해 살펴보도록 하겠다.

3.2 CMVP의 개념과 관련 표준의 구성 및 주요내용 분석

암호모듈에 대한 평가제도인 CMVP는 미 NIST(National Institute of Standards and Technology) 및 캐나다 CSE(Communication Security Establishment)가 1995년 공동 개발한 것으로서, 관련표준에 따라 암호모듈이 갖추어야 할 보안 요구사항 및 검증 요구사항을 제시하고, 이를 통해 암호모듈이 정보시스템의 보안성을 확보하는 데 적합한지를 평가하는 제도이다[9-10,16-17].

CMVP와 관련된 표준으로 NIST의 검증기준인 FIPS 140(폐지된 140-1, 현재 적용중인 140-2 및 신규 제정중인 140-3) 및 이를 기반으로 하는 시험기준인 DTR(Derived Test Requirements)이 있으며, FIPS 140 시리즈를 국제표준화한 ISO/IEC 19790 및 그의 DTR격인 ISO/IEC 24759 등이 있다[16-17]. FIPS 140-2 및 ISO/IEC 19790이 요구하는 내용은 상당히 유사한데, 암호모듈에 요구되는 4단계의 보안등급과 함께 이에 따른 요구사항을 11가지의 Category로 제시하고 있다[9-10]. 보안등급별 주요 내용과 Category의 명칭은 아래 및 Table 1과 같다.

- Security Level 1 : 가장 낮은 수준의 보안 등급으로서 기본적인 요구사항만을 포함한다.

- Security Level 2 : Lv.1에 더하여 아래와 같이 상향된 물리적 보안 메커니즘을 요구한다.
  * Tamper evident coatings or seals
  * Role-based Authentication
- Security Level 3 : Lv.2에 더하여 비인가 접근 시 대응 가능한 아래의 수단을 요구한다.
  * 구멍/틈새를 통한 침입 시도 검출기능
  * 비정상 환경(전압, 온도 등) 대응능력
  * ID 기반 인증 메커니즘
  * Tamper detection / response (zeroize 포함)
  * Life-Cycle Assurance
- Security Level 4 : 최상의 안전성을 제공하며, Lv. 1~3에 더하여 아래 사항을 추가 요구한다.
  * 외부전원 없이도 모든 물리적 접근 방어
  * 인지형(Password 등), 소유형(Token 등), 속성형(생체정보 등) 요소 중 2개이상 인증
  * 보다 상향된 환경조건 하에서도 침입 방지

Table 1. Categories of FIPS 140-2 & ISO/IEC 19790[9-10]

No.	FIPS 140-2	ISO/IEC 19790
1	Cryptographic Module Specification (same)	
2	Cryptographic Module Ports and Interfaces	Cryptographic Module Interfaces
3	Roles, Services, and Authentication (same)	
4	Finite State Model	Software / Firmware Security
5	Physical Security	Operational Environment
6	Operational Environment	Physical Security
7	Cryptographic Key Management	Non-Invasive Security
8	EMI / EMC	Sensitive Security Parameter Management
9	Self-Tests	
10	Design Assurance	Life-Cycle Assurance
11	Mitigation of Other Attacks (same)	

3.3 Anti-Tamper 개발 요구사항 도출

3.1절에서 암호모듈 및 무기 시스템의 공통점을 제시하였지만, 기본적으로는 두 시스템이 다르기 때문에 CMVP 표준에서 제시된 11가지 Category를 Anti-Tamper의 개발 요구사항으로서 그대로 적용하는 것은 적절하지 않다고 판단된다.

이에 무기 시스템의 Anti-Tamper 요구사항으로 적용이 불필요한 Category를 먼저 도출하고, 필수 또는 선택적으로 적용될 Category를 도출하였다. 그리고 CMVP 표준의 Category에 존재하지 않지만 무기 시스템에 필요한 요구사항을 추가 도출했다. 여기에는 한국산업표준으로 활용되고 있는 국제표준인 ISO/IEC 19790:2012(E)[9]을 활용하였다.

한편, 해당 표준에서 Anti-Tamper 개발 요구사항 적용이 불필요한 Category는 총 4가지이며, 이에 대한 판단근거는 아래와 같다.

- #1. Cryptographic Module Specification : 암호모듈의 유형(H/W, S/W 등) 및 동작 모드 등을 설시하는 것으로서, 이미 유형이 정해진 무기 시스템 개발에는 적용이 불필요하다.
- #4. Software/Firmware Security : S/W, Firmware 암호모듈의 무결성 확보 관련 요구사항이나, 현재도 무기 시스템 S/W요소에 대해 무결성 시험을 수행하고 있으므로 불필요하다.
- #7. Non-Invasive Security : 시스템의 중요정보 획득을 위한 직접적 침투에 대한 방어수단이 Anti-Tamper 이며, 이외의 침투에 대해 다루는 본 Category는 불필요
- #10. Life-Cycle Assurance : 방위사업관리규정 등에 따라, 모든 무기 시스템 개발 사업에 SE 절차가 적용되고 있으므로 중복적용 불필요

3.3.1 CMVP 표준에서 필수적으로 적용될 Anti-Tamper 요구사항 Category 도출

Anti-Tamper 적용이 결정된 모든 무기 시스템에 적용되어야 할 2가지 Category를 도출하였다.

- #3. Roles, Services, and Authentication : 무기 시스템의 운용 및 정비과정에서 S/W에 접근하는 모든 사용자는 '필요한 최저수준의 권한'만 보유해야 한다. 이 Category는 적정 등급의 권한을 보유하지 않은 자의 기술유출 시도를 방지할 수 있는 능력을 갖추기 위해 필요하다.
- #6. Physical Security : 무기 시스템의 H/W에 대한 Anti-Tamper 기법의 구현을 직접적으로 다루는 Category이다. 여기에 Tamper-Evident, Tamper-

Response, Tamper-Detection 및 Tamper-Response 등 전반적인 기법이 설시되어 있어 반드시 포함되어야 하는 것으로 판단하였다.
(Tamper-Evident는 Tamper-Detection과 Tamper-Deterrence 등이 중첩된 개념)

3.3.2 CMVP 표준에서 선택적으로 적용될 Anti-Tamper 요구사항 Category 도출

무기 시스템의 8대 분류유형 또는 기타 특성에 따라 Category 적용 필요성이 달라지므로, 아래와 같이 선택적으로 적용할 5가지의 Category와 함께 그 적용조건을 도출하였다.

- #2. Cryptographic Module Interfaces : 원격운용 가능한 무기 시스템의 경우에는 본 Category가 제시하는 데이터 및 제어 입·출력, 신뢰채널 등 요구사항이 반드시 필요하지만, 사용자가 직접 조작하는 무기 시스템에는 불필요하다.
(무기 시스템이 접속하는 군사용 네트워크에 보안 요구사항이 적용되었으므로 중복됨)
- #5. Operational Environment : 시스템 운영환경(플랫폼·구성요소 등의 H/W, 운영체제 관련 S/W)의 임의변경 가능여부에 따라 운영체제 적용이 필요한 요구사항을 제시하는 Category로서, 무기 시스템이 운영체제 등 S/W 요소를 포함하지 않은 경우 적용이 불필요하다.
- #8. Sensitive Security Parameter Management : 노출 시 보안이 손상되는 P/W 등을 지칭하는 CSP(Critical Security Parameter)와 공개키 등을 지칭하는 PSP(Public Security Parameter)를 일컫는 SSP에 대한 관리 요구사항으로서 거의 모든 무기 시스템에 적용이 필요하다. 다만, 예외적으로 특정 모듈과의 접속을 통해 기동하는 무기 시스템의 경우 해당 모듈에 SSP와 관련된 내용이 이미 반영되어 있을 가능성이 높다. 예를 들어 피아식별장치(IFF)에 적용된 연합암호자재는 특정한 암호 값 주입 없이는 기동되지 않으며, 이러한 암호 값은 SSP로서 특별히 관리되고 있다.
- #9. Self-Tests : BIT(Built-In Test)와 같은 자가 점검에 관련된 요구사항으로서, 이 Category는 “#5. Operational Environment”와 동일하게 S/W 요소를 포함하는 무기 시스템에 한하여 적용하는 것이 타당하다.
- #11. Mitigation of Other Attacks : 표준에 정의되지 않은 공격에 대한 대응기법이 적용되어 있는 경우에 한하여, 대응기법에 대한 명세 및 시험방법을 제시하여야 하는 요구사항이다. 즉, 표준의 범위를 벗어나 특별히 적용된 방어기법에 한하여 이 Category를 적용해야 한다.

3.3.3 무기 시스템을 위해 추가적으로 적용될 Anti-Tamper 요구사항 Category 도출

무기 시스템은 전투기능을 발휘하는 주장비 및 보조장비 뿐만 아니라, 전투발전지원요소 및 종합군수지원요소 등의 전력화지원요소까지 포함된다. 종합군수지원, 즉 ILS(Integrated Logistics Support) 요소는 무기 시스템의 운용을 위한 총 11가지의 요소들을 말하는데, Anti-Tamper 적용에 따라 기존 무기 시스템과 차별화된 ILS 요소 개발 및 평가가 수행되어야 한다. Anti-Tamper 관련사항의 반영이 필요한 ILS 요소는 아래의 3가지이다.

- 정비계획 : 무기 시스템에 적용된 Anti-Tamper 기법은 자칫 운영주체인 군의 정비과정에서 정비인력의 실수에 따라 발동되어 시스템의 일부 또는 전체 기능이 사용불능 상태로 전환되거나 훼손될 우려가 있다. 따라서 정비계획 수립 시 Anti-Tamper가 적용된 Subsystem 또는 Component 등에 대한 정비 단계별 적절한 수행범위를 반영하여야 한다.
- 군수지원교육 : 정비계획과 마찬가지로, 군의 정비인력에 대한 무기 시스템 관련 군수인력 모두에 대한 교육이 필요하다. 장비운용요원, 정비요원, 보급요원 등 모든 군수인력에 대한 공통교육사항 및 분류별 교육사항을 구분하여 군수지원교육 내용이 개발되어야 한다.
- 기술교범 : 군수지원교육 내용과 마찬가지로, 군수인력들이 Anti-Tamper 관련 내용을 계속 확인하기 위해서는 해당내용이 반영된 사용자 교범, 부대정비·야전정비·창정비 교범 등을 개발하여야 한다.

Anti-Tamper와 관련하여 도출한 개발 요구사항들을 정리하면, ISO/IEC 19790:2012 표준으로부터 2가지의 필수적용 항목과 5가지의 선택적용 항목, 4가지의 비적용 항목을 도출하였으며 추가적으로 ILS 요소 3가지를 도출하였다. 해당사항을 Table 2에 요약하였다.

Table 2. AT Requirement apply(From ISO/IEC 19790)

Classification	Category
Essential apply	#3. Roles, Services, and Authentication #6. Physical Security
Optional apply	#2. CM Interfaces #5. Operational Environment #8. SSP Management #9. Self-Tests #11. Mitigation of Other Attacks
Not apply	#1. CM Specification #4. Software / Firmware Security #7. Non-Invasive Security #10. Life-Cycle Assurance
Additional apply (ILS elements)	Maintenance Planning Logistics Training Technical Drill Book

3.4 Anti-Tamper 요구사항 활용 방안 도출

연구개발주관기관은 무기 시스템의 개발 초기단계부터 3.3절에서 도출한 Anti-Tamper 개발 요구사항들을 적절하게 활용하여 시스템 개발활동을 수행할 수 있다. 또한 방위사업청의 지침에 따라 무기 시스템 연구개발사업은 시스템공학 절차에 따라 관리되고 있으므로 각 기술검토회의를 통해 무기 시스템에 적용될 Anti-Tamper 기법들이 기술유출을 방지하는 데에 충분한지, 혹 무기 시스템의 운용성을 저해하지는 않는지 등을 검토할 수 있다.

무기 시스템의 개발 프로세스 상, 체계개발단계 후반부에는 설계된 시스템 시제품의 검증을 위한 개발시험평가(DT&E)와 무기 시스템의 전투임무적합성 여부를 확인하는 운용시험평가(OT&E)를 수행한다. 정확하고 객관적인 시험평가의 수행을 위해서는 시스템 개발 요구사항을 토대로 도출된 시험 요구사항이 필요한데, 이 경우 역시 CMVP 표준을 활용할 수 있다.

CMVP의 국제표준인 ISO/IEC 24759:2017(E)는 개발하려는 암호모듈이 ISO/IEC 19790:2012(E)의 11가지 Category의 요구사항을 만족하는지에 대한 시험항목과 절차 등을 다루는데, Anti-Tamper 개발 요구사항과 동일하게 시험평가를 위한 검증 요구사항으로 활용이 가능할 것으로 판단된다.

4. 귀납추론 및 비교평가를 통한 제시방안의 유용성 및 타당성 확인

3장에서 도출하여 제시한 'CMVP 표준 기반의 Anti-Tamper 개발 요구사항과 활용방안'은, 아래에 제시하는 근거를 사용한 인과적 귀납 추론을 통해 그 유용성이 존재하는 것으로 판단할 수 있다.

- 3.1절에서 제시한 바와 같이, 무기 시스템과 암호모듈 사이에 상당한 공통점이 존재한다.
- CMVP 표준은 상당기간 세계적으로 사용되어 그 유용성이 인정되며, 동 표준의 적용을 통해 암호모듈은 '중요정보 유출 대응능력'을 보유하도록 개발 및 평가되고 있다.
- 따라서, 무기 시스템은 CMVP 표준 기반 Anti-Tamper 요구사항을 통해 '중요기술 유출 대응능력'을 보유하도록 개발 및 평가될 수 있다.

연구수행 결과의 타당성을 강화하기 위해 무기 시스템의 수명주기적 관점에서 기술보호 활동의 효율성에 대한 비교평가를 수행하였다. 평가대상은 아래의 3가지이다.

- #1. 현 방위산업기술보호 제도만을 적용
- #2. 선행연구[6-7]에서 제시된 적용방안
- #3. 제안방안(CMVP 기반의 요구사항 적용)

비교평가 기준으로, 연구수행 목표를 포함하여 아래의 총 5가지를 선정하였다.

- #1. 무기 시스템이 Tampering 등의 기술유출 시도로부터 보호될 수 있는가?
- #2. 기술보호 목표를 위해 적절한 Anti-Tamper 기법을 선택하는 Framework가 있는가?
- #3. 개발자들은 무기 시스템 내에 Anti-Tamper 기법을 효과적으로 적용할 수 있는가?
- #4. 무기 시스템에 적용된 Anti-Tamper 기법을 객관적, 효과적으로 평가할 수 있는가?
- #5. 무기 시스템의 운영·유지 단계에서, Anti-Tamper 기법의 오작동을 예방할 수 있는가?

비교평가 수행 결과 Table 3과 같이 방안 #1은 기준 충족이 불가능하며 방안 #2는 제한적으로만 충족 가능한 반면, 연구결과로 제시한 방안 #3은 주어진 기준을 모두 충족하는 것으로 평가된다.

Table 3. Results of Comparative Evaluation

Evaluation element	#1	#2 (Precedent studies)	#3 (Proposed)
Does the Weapon system have capability to protect itself from Tampering?	X (No Security strategy for Weapon systems)	○ (The Anti-Tamper techniques)	○ (The Anti-Tamper techniques)
Is there a Framework for selecting the appropriate Anti-Tamper techniques?		△ (Only for PMs, not for developers)	○ (Selectional apply of ISO/IEC 19790)
Can developers effectively apply the Anti-Tamper techniques to Weapon system?		△ (Not linked with Life-cycle Process)	○ (Selectional apply of ISO/IEC 19790)
Can be the applied Anti-Tamper techniques evaluated objectively and effectively?		X (Not considered)	○ (Selectional apply of ISO/IEC 24759)
On the "Operation & Maintenance" stage, Can be the Malfunction of Anti-Tamper techniques prevented?		X (Not considered)	○ (ILS elements, such as Tech. Drill book)

5. 결 론

본 논문에서는 무기 시스템 획득 프로세스에서 효율적인 Anti-Tamper 적용을 위해 개발 및 검증 요구사항을 도출하였다. 요구사항 도출에 활용된 CMVP 표준은 암호모듈이 정보시스템의 보안성을 확보할 수 있도록 하는 데에 필요한 개발 및 검증 요구사항이며, 국제표준인 ISO/IEC 19790의 11개 Category 중에서 무기 시스템과의 공통점 및 차이점을 고려하여 Anti-Tamper 개발 요구사항으로서 활용할 수 있는 항목들을 도출하였다. 이와 더불어 종합군수지원(ILS)요소 중 Anti-Tamper의 적용에 따라 특별히 개발해야 할 요소들을 도출하였다.

귀납추론 및 비교평가를 통해 논문에서 제시한 방안이 연구목표를 달성하였으며 본 연구결과가 유용한 것으로 판단하였다. 이로서 국내개발 무기 시스템의 수명주기 관점의 기술보호에 도움이 될 것으로 판단된다.

향후에는 이러한 Anti-Tamper 개발 요구사항을 바탕으로 무기 시스템 개발과정에서 시범적용 등 추가적인 연구 수행을 통해 더욱 효율적인 무기 시스템 기술보호 방안이 마련되어야 하겠다.

References

[1] H. J. Lee, "On the development of an Effective Defense Technology Security System," Defense & Technology, Korea Defense Industry Association, Nov. 2017, vol. 465.

[2] *Department of Defense DIRECTIVE : Anti-Tamper(AT),* DoD Directive 5200.47E, 2015.

[3] M. C. Park, W. K. Koo, D. G. Suh, I. S. Kim, D. H. Lee, "Two-stage tamper response in tamper-resistant software," IET Software, Vol. 10, No. 3, pp. 81-88, 2016.
DOI : http://dx.doi.org/10.1049/iet-sen.2014.0231

[4] M. H. Jang, Y. S. Ryu, H. K. Park, "A FPGA-Based scheme for protecting weapon system software technology," in Proc. ICCSA 2018, Melbourne, VIC, Austrailia, Jul. 2-5, 2018, pp. 148-157.
DOI : https://doi.org/10.1007/978-3-319-95174-4_12

[5] Mikhail J. Atallah, Eric D. Bryant, and Martin R. Stytz, "A survey of anti-tamper technologies," CROSSTALK : The Journal of Defense Software Engineering, vol. 17, no. 11, pp. 12-16, 2004.

[6] H. K. Lee, W. S. Lee, Y. J. Oh, S. S. Park, "A Trend Analysis and Technology Application of Defense Technology Protection," Journal of the KIMST, Vol. 20, No. 4, pp. 579-586, 2017.
DOI : http://dx.doi.org/10.9766/KIMST.2017.20.4.579

[7] H. S. Chae, C. S. Lee, T. R. Kim, T. H. Kim, "The Design of the Response Method in Anti-tampering for UGV," in Proc. 2017 KIMST Fall Symposium, Daejeon, Republic of Korea, Nov. 14-15, 2017, pp. 819-820.

[8] M. W. Lee, J. C. Lee, "Risk Management-Based Application of Anti-Tampering Methods in Weapon Systems Development," Journal of KAIS, Vol. 19, No. 12, pp. 99-109, 2018.
DOI : https://doi.org/10.5762/KAIS.2018.19.12.99

[9] *Information technology — Security techniques — Security requirements for cryptographic modules*, ISO/IEC Standard, 19790, 2012.

[10] *Security requirements for cryptographic modules*, FIPS PUB 140-2, 2001

[11] S. J. Ahn, C. K. Jung, K. S. Oh, J. Y. Lee, "A Study on the Development of Defence Technology Protection System," Sungkyunkwan Univ. Univ-Industry Collabo,

Director General for Defense Technology Control of DAPA, Oct. 2016.

[12] *Department of Defense Instruction : Critical Program Information(CPI) Protection Within the Department of Defense*, DoD Instruction 5200.39, 2008.

[13] United States Government Accountability Office, "DoD Needs to Better support program managers' implementation of AT protection," GAO-04-302, Mar. 2004.

[14] United States Government Accountability Office, "Department-wide Direction Is Needed for Implementation of the Anti-tamper Policy," GAO-08-91, Jan. 2008.

[15] *Statement of Anti-Tamper(AT) Measures in the Letter of Offer and Acceptance(LOA)*, DSCA 00-07, 2000.

[16] M. G. Choi, J. H. Jeong, "A Study on the Policy of Cryptographic Module Verification Program," Journal of KAIS, Vol. 12, No. 1, pp. 255-262, 2011.
DOI: https://doi.org/10.5762/KAIS.2011.12.1.255

[17] K. S. Kou, I. W. Bae, S. J. Choi, G. S. Lee, "Analysis on New Cryptographic Module Validation Standard FIPS PUB 140-3 Changes," Review of KIISC, Vol. 17, No. 6, pp. 41-56, 2007.

이 민 우(Min-Woo Lee) **[정회원]**

- 2008년 3월 : 해군사관학교 전기공학과 (공학사, 군사학사)
- 2014년 2월 : 한국외국어대학교 태국어과 (문학사)
- 2014년 2월 : 국민대학교 정치대학원 (정치학석사)
- 2015년 7월 ~ 현재 : 방위사업청 획득전문형 장교 (해군소령)
- 2016년 9월 ~ 현재 : 아주대학교 시스템공학과 (박사과정)

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), 기술보호, 요구공학 (RE), 방위력개선사업, Weapon Systems R&D

이 재 천(Jae-Chon Lee) **[정회원]**

- 1977년 2월 : 서울대학교 공과대학 전자공학과(공학사)
- 1979년 2월 / 1983년 8월 : KAIST 통신시스템 (석/박사)
- 1984년 9월 ~ 1985년 9월 : 미국 MIT Post Doc 연구원
- 1985년 10월 ~ 1986년 10월 : 미국 Univ. of California 방문연구원
- 1990년 2월 ~ 1991년 2월 : 캐나다 Univ. of Victoria (Victoria, BC) 방문교수
- 2002년 3월 ~ 2003년 2월 : 미국 Stanford Univ. 방문교수
- 1994년 9월 ~ 현재 : 아주대학교 시스템공학과 정교수

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), Systems Safety, System T&E, Modeling & Simulation