정 보 보 호 학 회 지
제28권 제6호, 2018. 12

방위산업기술 보호기법 적용 연구

이 효 근* **, 이 운 순*

요 약

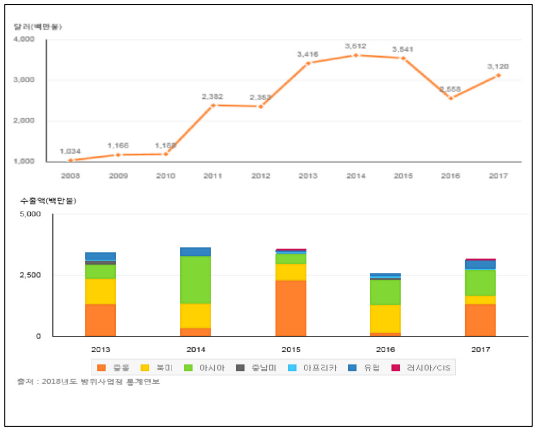
군사력은 국가경쟁력을 대표할 수 있는 가장 중요한 요소 중 하나이다. 세계 각국에서는 군사력 증진을 위한 군사장비의 수출과 수입이 활발하게 이루어지고 있다. 우리나라의 방산수출은 2006년 2.5억불에서 2017년 약 12배 증가한 31.2억불로 2011년부터 6년 연속 20억불 이상 성과를 달성하였으며 방위산업 수출은 탄약·부품류 위주의 수출에서 첨단 기술력에 기반을 둔 고부가가치 무기체계로 수출품목이 다양화 되고 있다. 이렇듯 우리나라도 이제 방위산업 기술보호에 대한 관심과 노력이 반드시 필요한 시기가 도래하였다. 본 연구에서는 수출 시 또는 적의 피탈에 의해 무기체계가 노출되는 상황에서 핵심기술의 유출을 방지하기 위한 기술보호기법에 대해 조사하고 실제 무기체계에 적용하여 구현하였다.

Ⅰ. 서 론

우리나라의 방산수출액은 2006년 2.5억불에서 2017년 약 12배 증가한 31.2억불로 2011년부터 6년 연속 20억불 이상 성과를 달성하였으며 방위산업 수출은 탄약·부품류 위주의 수출에서 첨단 기술력에 기반을 둔 고부가가치 무기체계로 수출품목이 다양화 되고 있다. 근래의 주요 수출품으로는 K-9 자주포 및 T-50고등 훈련기와 같은 첨단화 된 장비 등 있다. 그림 1에서와 같이 권역별로도 전통 수출 대상지역인 아시아, 중동 외에 유럽, CIS 및 아프리카 국가에 대한 신규시장 개척으로 수출지역이 다변화 되고 있다.

수출의 증가를 통해 국내 무기체계의 기술이 부당변경(Tampering)에 의해 노출 될 수 있는 위험도 늘어나게 된다. 따라서 수출 또는 적의 피탈에 의해 의도하지 않은 핵심기술의 이전이나 무기체계의 불법 개조 및 역공학에 의한 대응장비 개발 등을 방지하기 위해 무기체계에 대한 방산기술 보호 조치가 선행되어야 한다. 국내에서는 이러한 움직임에 따라 방위산업 기술보호법이 재정되었으며 기술보호 대상 핵심기술 도출 사업 등이 수행되고 있다.

본 연구에서는 일반적인 기술보호기법에 대한 조사와 분석을 수행하였으며, DOD의 ATEA (Anti-Tamper Executive Agency) 정책인 Anti-Tampering 결정 프로세스를 분석하여 연구개발 시 적합한 기술보호기법을 선정하고 적용하였다.



〔그림 1〕 Actual Results of Defence Export

Ⅱ. 본 론

2.1. 연구대상 장비 선별

본 연구에서는 향후 수출가능성이 높으며 적의 피탈이나 전투 중 손실되어 부당변경 가능성이 있거나 대응장비를 개발할 가능성이 있고 HW 및 SW가 함께 적용

본 연구는 ㈜한화/방산 종합연구소의 관리로 수행되었습니다.
* ㈜한화/방산 종합연구소 (hyokeun84@hanwha.com)
** 고려대학교 기계공학부 (hyokeun84@korea.ac.kr)

되어 주요 핵심기술 및 군사적 운용개념이 적용된 무기체계에 대한 분석과 선별을 수행하였다. 선별결과 현재 야전에 배치되어 사용 중인 지능형 지뢰체계 중 하나를 선별하였으며 보호하고자 하는 대상 및 기술은 기폭 알고리즘 및 센서가 내장된 회로카드조립체 및 SW로 선정하였다.

2.2. 연구대상 기법 분류

기술보호기법의 분류에는 여러 가지 방법이 있지만 본 연구에서는 HW적인 보호기법과 SW적 보호기법으로 구분하였다. 또한 기술의 적용영역을 감지, 억제, 방지, 반응 의 수준으로 구분하였다.

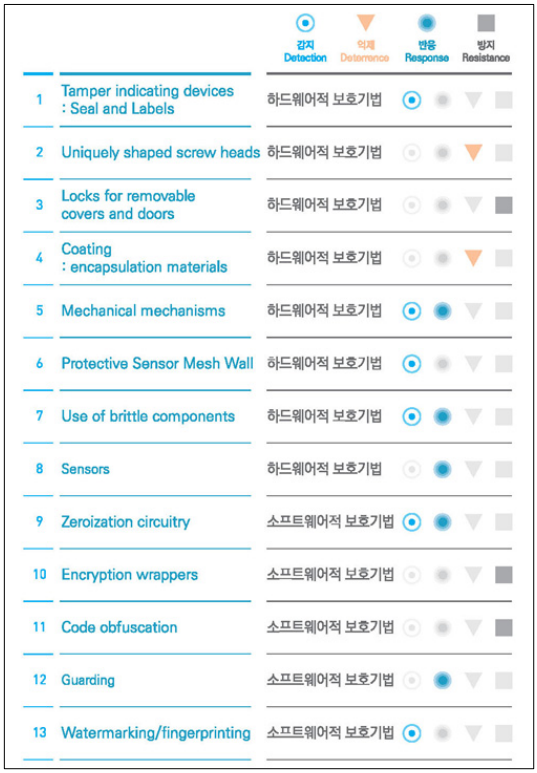
방산분야의 핵심기술 보호기법은 주요 보안사항으로 널리 알려져 있지 않다. 따라서 본 연구에서는 그림 2에 나열한 민수분야에 널리 사용되는 일반적인 기술보호기법 13종(HW8종, SW 5종)을 조사하여 식별하였다. 각각의 기술보호기법의 종류 및 구성은 감지 억제 반응 방지 4종의 적용영역을 바탕으로 HW 및 SW에 각각 적용 가능한 기술로 분류하였다.

2.3. 부당변경 방지 프로세스

2.3.1. DOD Anti-Tampering 프로세스

미국은 ATEA(Anti-Tamper Excutive Agency)를 설치하여 정책을 실행하고 무기체계 개발 시 핵심기술이 사용된 모든 신규 또는 성능개량 사업의 요구사항에 대하여 부당변경 방지법을 단계적으로 결정하고 수행하고 있다.[1],[2] 본 연구에서는 DOD의 Anti-Tampering 결정 프로세스를 바탕으로 총 10단계의 과정을 거쳐 기술보호기법 대해 분석 및 적용하는 과정을 수행하였다.

DOD의 Anti-Tampering 결정 프로세스는 무기체계에 적용된 핵심기술을 보호하기 위한 일련의 과정으로 내용은 다음과 같다. 먼저 대상핵심기술을 파악한 후 위험요소와 취약점을 분석한다. 그 후 공격 예상 시나리오를 통해 부당변경이 가능한 충격을 파악하고 이를 최소화 할수 있는 방안을 찾는다. 이후 이용 가능한 기술보호 기법을 파악한 후 가능한 구현방법을 선택한다. 최종적으로 기술에 대한 구체적 문제를 파악 후 해결책 단계에 포함하여 적용한다.[3],[5],[6] 이러한 부당변경 방지 10단계의 과정을 거쳐 핵심기술 유출 위험 식별 및 기술보호 대책을 마련할 수 있다.



〔그림 2〕 General technology protection techniques

2.3.2. Anti-Tampering 적용

본 연구에서는 다음과 같이 Anti-Tampering 프로세스를 적용하였다. Anti-Tampering 프로세스는 해당 과제 또는 제품에 방산기술이 필요한지에 대한 분석과정을 수행한 이후 적합한 방산기술을 선정 및 적용하는 두 가지 큰 카테고리로 구분된다.

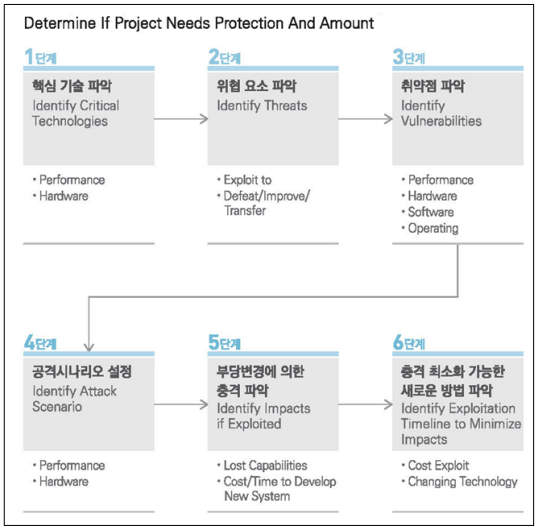
2.3.2.1. 프로젝트 및 제품의 보호여부 판단

1단계 핵심기술 파악 : 지능형 지뢰체계의 HW인 회로카드 조립체 내장 SW를 주요 핵심기술로 파악.

2단계 위협요소 파악 : 핵심기술의 노출 및 탈취.

3단계 취약점 파악 : 회로카드조립체에 대한 접근은 현재 무방비 상태이며 SW 접근이 용이함.

4단계 공격시나리오 설정 : 수출국 혹은 적군의 피탈



〔그림 3〕 Determine if project needs protection and amount

에 의한 부당변경 시도.

5단계 부당변경에 의한 충격 파악 : 기술유출 시 적국의 대응방안 마련을 통한 무기체계의 무력화.

6단계 충격 최소화 가능한 새로운 방법 파악 : 기술유출 시도 시 접근방지 혹은 접근 후 탈취 불가한 상태 전환

2.3.2.2. 적합한 보호기법 선정 및 적용

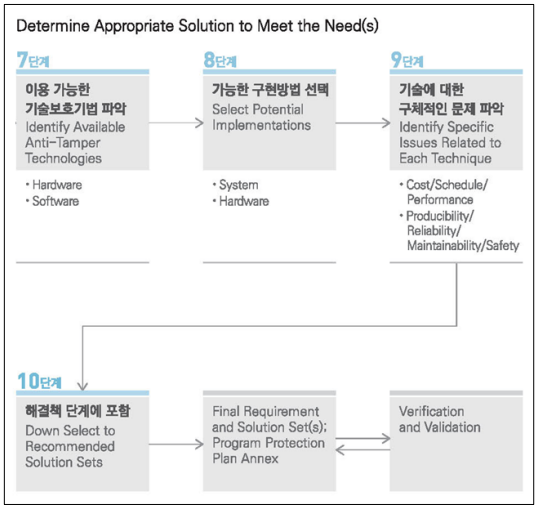
7단계 이용가능한 기술보호기법 파악 : 그림 2의 13가지 일반적인 기법 중 HW의 접근을 방어하는 1, 2, 4, 5번 기법과 SW의 접근을 방지하는 8, 9번 기법이 본 무기체계에 적용하기에 비용 대 효과가 가장 뛰어난 것으로 분석. 접근권한인증을 통한 피아식별 기능을 추가 적용 가능한 것으로 분석.

8단계 가능한 구현방법 선택 : 7단계에서 선별한 기술보호기법을 접근 단계별 적용. (분해, 탈취, 변경)

9단계 및 10단계는 본 논문에서 적용한 기법을 실제로 운용한 이후에 반영할 수 있는 영역이므로 본 논문에서는 다루지 않았으며 이후 연구영역에서 다룰 예정이다.

2.4. 기술 보호기법 적용

본 연구에서는 선정된 대상 장비에 2.3절에서 다룬



〔그림 4〕 Determine Appropriate solution to meet the Need(s)

일반적인 기술보호 기법 중 6가지의 기법과 독자적으로 고안한 1가지의 기법 등 총 7가지 기술보호기법을 시스템의 운용방안에 맞추어 통합하였다. 각 기술보호기법은 독자적으로 운용이 가능한 설계이며 시스템, 조립체, 구성품의 단계에 따라 구분하고 대상 장비 시스템에 통합설계를 수행하였다.

2.4.1. 시스템 기술보호기법

2.4.1.1. 권한인증기법

시스템 권한인증기법은 시스템 단위에 접근자의 피아를 식별하여 아군일 경우 시스템에 대한 권한인증을 부여하여 접근이 가능하도록 한다. 적군일 경우 부당변경이 시도되지 못하도록 제어하는 기법으로 시스템 단위의 감지 및 반응의 역할을 수 행한다. 본 기법의 구성품으로는 대상무기체계인 기술보호 구현장치 내부의 RFID 인식기 등이 포함되어 있으며 사용자가 소유하도록 된 기술보호 권한장치와(RFID 태그) 제어모드 설정을 할 수 있는 기술보호 제어장치로 구분된다. 본 기법은 총 5대의 기술보호 구현장치와 권한장치를 통신의 충돌 없이 운용하도록 다중화 시스템으로 설계되었다. 리더는 시분할 다중방식이며 기술보호 구현장치는 ISO/IEC 1900-7 규격에 정의된 Dynamic Framed Slotted Aloha 방식을 사용하였다. [4]

기술보호 제어장치는 기술보호 구현장치를 인코딩하고 제어하며, 기술보호 구현장치와 기술보호 권한장치가 피아식별정보를 활용하여 기폭을 제어하고 피아식별정보를 기술보호 제어장치로 무선 전송한다. 비인가 접근자의 접근을 감지하고 기술보호 구현장치 혹은 제어장치가 반응하여 시스템으로의 접근을 방지한다.

2.4.1.2. 접근억제기법

본 기법은 'Tamper Indicating Devices'를 활용한 방안으로 민수 또는 군수에서 널리 사용되는 방식으로 비인가자가 기술보호장치에 사전 접근하지 못하도록 하는 방법으로 부당변경의 감지 및 억제를 수행한다. 억제장치가 설치되어 있음을 인지하거나 Seal 또는 Label을 적용하여 법적조치 등의 제지 문구를 삽입하여 사용자에게 주의를 주고 접근을 차단한다.

본 연구에서는 전용 Seal과 Label을 연구 대상 장비에 가장 적합한 형태와 색상으로 제작하여 시각적 인 효과를 높이고 시스템의 기술유출시 반드시 분해가 필요한 부분을 분석한 후 최적의 위치를 선정하여 경고성 억제문구를 부착하였다. 이에 따라 시스템 시도 시 접근

〔그림 5〕 Selected technology protection techniques

억제를 요하는 경고성 문구를 모든 상황에서 확인 할 수 있으며 인지에 따른 분해의 방지효과를 기대할 수 있다.

2.4.2. 조립체 기술보호기법

2.4.2.1. 접근억제기법

본 기술보호기법은 기술보호 구현장치의 기구적 기술보호기법으로 부당변경 시도 시 특수한 볼트헤드를 적용한 조립체의 분해를 지연시키는 역할을 수행하며 'Uniquely Shaped Screw Head' 방안의 한 종류이다.

본 연구에서는 볼트의 형상변경을 통해 부당변경을 효과적으로 억제할 수 있는 방법으로 특별한 형태의 특수공구를 제작하여 대상 장비에 적용하였다. 이를 통해 시스템 비인가자의 접근 시 전용 공구의 부재로 시스템의 접근을 차단 혹은 지연시킬 수 있는 효과를 기대할 수 있다.

2.4.2.2. 접근반응기법

휴대용 전원을 사용하는 무기체계는 전원이 제거되면 접근반응 기법이 작동하지 않게 된다. 따라서 본 연구에서는 'Mechanical Mechanisms' 기법을 활용하였으며 시스템 접근이 감지되면 자동으로 전원이 활성화되는 장치를 개발하여 휴대용 전원과 상관없이 동작 가능한 기술보호기법을 개발하였다.

일반적으로 전원을 활성화시키는 기술은 무기체계의 특성(회전, 관성력, 탄성 등)을 이용하여 열전지나 앰플형 전지를 활성화시키는 기술이 사용된다. 하지만 특정 외력이 존재하지 않는 대상무기체계의 경우 이를 활용하기 어렵기 때문에 시스템 분해 시 기존 전지와는 기구적으로 분리되어 있는 별도의 전력을 활용하는 기법을 적용하였다.

주 전원이 삽입되어 있을 시 보조전원 장치의 전 원이 비활성되며 주 전원을 제거 시 보조전원이 활성화되는 기법으로 흔히 공공장소의 비상용 손전등에 사용되는 기술과 유사하다. 이를 통해 시스템의 이상 접근자의 전원 제거 시도를 감지하고 전원 제거 시 시스템이 반응할 수 있도록 하여 기술유출에 대한 방지효과를 기대할 수 있다.

2.4.3. 구성품 기술보호기법

2.4.3.1. 접근방지기법

본 기법은 몰딩 혹은 코드명 삭제 등의 조치를 통해 회로카드 혹은 전자부의 식별을 어렵게 하여 비인가자의 시스템 접근을 지연 혹은 방지시키는 기법으로 'Coating' 기법을 활용하였다. 운용알고리즘이 탑재된 CPU는 코팅 또는 몰딩하여 내부의 SW에 대한 접근을 방지할 수 있다. 전자 제품의 제품명을 삭제하여 SW를 역공학 혹은 부당변경 시 지구상에 알려진 모든 CPU 명령코드를 이용해 바이너리 파일을 해독 하여 CPU의 종류를 파악해야 하며 이는 현실적으로 진 행이 어려운 방안이다. 임베디드에서 많이 사용되는 코어는 ARM, Atmega, PIC, 8051 등이 있으며, 기타 PowerIC, Motorola, Intel, Freescale, Hitachi 등 많은 코어가 존재하기 때문에 역공학 혹은 부당변경등의 인가되지 않은 무기체계의 접근에 최대 10배 이상의 시간이 소요되게 된다.

2.4.3.2. HW 접근반응기법

본 기술은 'Sensor'에서 소개한 기술을 활용한 것으로 무기체계 내부에 근적외선 센서를 장착하여 사람의 접근 혹은 빛에 반응하도록 설계를 구현하였다. 기술보호 구현장치가 부 당변경에 의해 감지 시 핵심기술이 포함되어 있는 구성품에 과전류를 흘려 해당 구성품을 파괴하여 정상적으로 작동하지 못하게 하는 HW 접근반응 기술보호기법을 개발하여 적용하였다. 기술보호 구현장치에서 CPU는 운용알고리즘을 내장하고 있는 구성품으로서 권한인증 되지 않은 접근자에 의해 조립체가 분해되면 구성품의 특정 단자에 전원을 직접 인가하여 구성품을 파괴시켜 운용 알고리즘의 접근을 차단한다.

2.4.3.3. SW 접근반응기법

무기체계는 다양한 분류에 따라 작동할 수 있또록 내부에 SW를 탑재하고 있다. SW는 무기체계의 작동원리를 포함하는 핵심기술로 SW를 보호하기 위해 리소스 암호화, 소스코드 난독화와 바이너리코드 난독화 같이 HW의 변경없이 방산기술 보호기법의 적용이 가능한 장점을 가지고 있다.

본 기법은 HW 접근반응기법에서 적용한 근적외선 센서의 감지모드를 활용하여 부당변경 및 비인가 접근을 감지한다. 또한 'Zeroization Circuitry' 기법을 활용하여 기술보호 구현장치가 부당변경에 의해 감지가 되면 핵심기술이 포함되어 있는 CPU의 데이터를 모두 '0'으로 포맷하여 SW의 역공학을 방지하는 기법을 적용하였다. 이를 통해 시스템에 인가되지 않은 사용자의 부당한 접근을 감지 시 시스템 내부로의 접근을 차단하고 대상 시스템을 무능화하여 부당한 접근을 통한 기술유출을 방지할 수 있다.

Ⅲ. 결 론

본 연구는 방산기술 보호기법 적용에 대한 시범 연구로 Anti-Tampering 결정 프로세스를 기반하여 방산 기술 보호기법을 적용한 국내 최초의 기술보호 기법 연구이다. 본 연구는 수출 또는 적의 피탈에 의해 원치 않는 핵심기술의 이전이나 무기체계의 불법 개조와 역공학에 의한 대응장비 개발 등을 방지하기 위해 무기체계의 핵심기술 위협요소 및 취약점을 분석하고 방산기술을 보호하기 위한 기법을 개발하였다.

본 연구에서 개발된 7가지 기술보호기법은 8대 무기체계에 대한 적합성을 분석하여 선별적으로 적용할 수 있다. 특히 7가지 기술 중 시스템 접근억제, 조립체 접근억제, 구성품 접근방지, SW 접근반응 기법 등 4가지 기술보호기법은 8대 무기체계 대부분에 큰 비용의 소요없이 즉각적으로 적용 가능할 것으로 분석된다.

본 연구에서는 일반적인 기술보호기법에 대한 분석결과를 무기체계에 적용가능 하도록 개발하였으나 기술보호기법 자체를 핵심기술로 분류하여 주요 핵심기술에 대한 보호장치를 구축하여야 한다. 향후 8대 무기체계에 대한 다양한 기술 분석을 통해 핵심기술로 분류된 기술에 대한 보호기법 및 제도를 구축하여야 한다. 또한 주요무기체계 개발 시 기술보호기법을 사업초기부터 선별 적 적용하여 부당변경을 통한 기술유출 및 무기체계 대응에 대한 대책을 수립하여야 한다. 이를 위해 무기체계 개조개발 지원 프로그램을 통해 예산을 지원해 주는 제도를 통해 무기체계별 핵심기술개발 사업과 같은 연구개발 과정을 도입하고 방산기술 보호기법에 적용을

사례를 확대하여 기술보호에 대한 인식개선 및 참여를 이끌어야 한다.

참 고 문 헌

[1] Dr. Mikhail J. Atallah, Eric D. Bryant, and Dr. Martin R. Stytz, “A survey of Anti-Tamper Techologies”, CROSSTALK The Journal of Defense Software Engineering, pp. 13-16, November 2004.

[2] Gansler, J. S, “Implementation of anti-tamper (AT) techniques”, DoD memorandum, March 1994.

[3] Anderson, R, and M. Kuhn, “Tamper Resistance - A Cautionary Note. Proc.of Second Usenix Workshop on Electronic Commerce”, Oakland, CA, pp. 1-11. Nov. 1996.

[4] Arbaugh, W, D. Farber, and J. Smith, “A Secure and Reliable Bootstrap Architecture. Proc. of the IEEE Symposium on Security and Privacy”, Oakland, CA, 1997.

[5] Lt Col Art Huber, Jennifer M. Scott, “The Role and Nature of Anti-Tamper Techniques in U.S. Defense Acquisition 357”, Acquisition Review Quarterly, Fall 1999.

[6] Alvaro Ortega Chamorro, “Physical Protection : Anti-Tamper mechanisms in CC security evaluations”, EPOCHE & ESPRI, Norway, 10ICCC.

〈저 자 소 개〉

이 효 근 (Lee Hyo Keun)
2010년 2월 : 고려대학교 기계공학 학사 (졸업)
2012년 2월 : 고려대학교 기계공학 석사 (졸업)
2012년 1월~현재 : ㈜한화 종합연구소 선임연구원 (재직)
2015년 3월～현재 : 고려대학교 기계공학과 박사과정 (수료)
관심분야 : 기계공학, 무선통신, 센서, 정보보호

이 운 순 (Lee Woon Soon)
2000년 2월 : 충남대학교 전파공학 학사 (졸업)
2002년 2월 : 충남대학교 전파공학 석사 (졸업)
2002년 2월~2010년 5월 : GCT semiconductor
2010년 6월～현재 : ㈜한화 종합연구소 책임연구원 (재직)
관심분야 : 체계공학, 정보통신, 방산기술보호 연구