사이버전을 대비한 무기체계의 보안시스템 구축 방안

이용준*, 박원형*
*극동대학교 사이버보안학과
e-mail:2020032@kdu.ac.kr, whpark@kdu.ac.kr

Security System for Weapon System in preparation for Cyber Warfare

Yong-Joon Lee*, James Park*
*Dept. of Cyber Security, Far East University

요 약

국방 분야의 무기체계는 SW에 대한 취약점 점검 및 소프트웨어 개발과정에서 사이버전에 위협에 대응하는 준비가 수행되고 있다. 그러나 미국, 이스라엘에 대비하여 국내 무기체계를 대상으로 하는 보안시스템을 통한 관제 등은 실시되지 못하는 한계를 가지고 있다. 이에 본 논문에서는 해외 무기체계 사이버보안 시스템을 분석하여 국내에도 무기체계에 사이버보안 시스템을 도입이 필요하다는 당위성과 사이버전에 대응이 가능하도록 제안한다.

1. 서론

국방 분야의 무기체계는 SW에 대한 취약점 점검 및 소프트웨어 개발과정에서 사이버전에 위협에 대응하는 준비가 수행되고 있다. 그러나 미국, 이스라엘에 대비하여 국내 무기체계를 대상으로 하는 보안시스템을 통한 관제 등은 실시되지 못하는 한계를 가지고 있다. 이에 본 논문에서는 해외 무기체계 사이버보안 시스템을 분석하여 국내에도 무기체계에 사이버보안 시스템을 도입이 필요하다는 당위성과 사이버전에 대응이 가능하도록 제안하였다.

2. 무기체계 SW 기술 분류

내장형 SW는 마이크로프로세서 위에 내장되어 제한된 자원을 최적으로 활용하여 특정 기능을 수행하도록 지원하는 소프트웨어를 총칭한다고 할 수 있다. 즉 정보가전, 자동차, 항공기 등 다양한 산업분야의 제품에 내장되어 시스템을 제어하고, 특정 목적을 수행하는 소프트웨어이다. [표 1]과 같이 이러한 내장형 SW의 적용범위는 매우 광범위하고 그 영역을 급속도로 확대해 나가고 있다.내장형 SW는 '미리 정의된 목적을 위해 물리적 입력 및 그 가공된 데이터를 이용하여 적절한 반응을 제공하기 위해 맞춤 설계된 소프트웨어' 라고 정의할 수 있다. 내장형 SW는 스마트 가전과 같은 첨단 산업이나 국방과 같은 특수 산업을 포함한 다양한 산업과 결합하여 부가가치를 향상하는 기술로 다음과 같은 특성을 갖는다[1].

- 실시간성(Real-time) : 멀티미디어 스트림, 산업 제어기기 등에 탑재되어 제한시간 내 정확한 작업과 서비스를 제공할 수 있어야 한다.
- 이질성(Heterogeneity) : PC와 같은 범용 장비에서는 범용 운영체계를 통해 서로 다른 기능을 갖는 다양한 소프트웨어가 실행된다. 반면 내장형시스템에서는 특정 목적에 특화된 내장형 SW만 작동한다. 다른 내장형시스템에서는 그 시스템에서 요구하는 또 다른 목적의 내장형 SW가 운영된다.
- 고성능성(High-performance) : 하드웨어 성능의 비약적인 발전과 3D 응용, 증강현실 등 높아진 사용자 요구사항으로 인해 다양하고 풍부한 고속 응용의 지원이 필요하다.
- 고신뢰성(High-assurance) : 국방, 항공, 차세대 네트워크, 자동차 등 시스템 오류나 오동작으로 인해 환경적으로 큰 피해를 입을 수 있는 분야에 적용되어 고장에 대해 감내할 수 있는 기능을 제공하여야 한다.
- 경량화(Light-weighted) : 센서와 같은 소형, 초소형 기기 제품에 탑재하기 위해 내장형 SW의 크기 최소화 기능을 지원하여야 한다
- 생존성(Liveness) : 열약한 환경의 산업 현장이나 군사 응용에서는 먼지, 바람, 습기, 기온의 변화와 같은 악조건에서도 잘 작동할 수 있도록 패키징하는 기술을 제공하여야 한다.

• 자원 및 환경의 제약(Constraints) : 저전력화가 대표적인 케이스이다. 부족한 리소스를 최대한 활용할 수 있는 기술의 개발과 하드웨어시스템과 사용자 패턴 등을 잘 파악하여 에너지 효율적으로 시스템을 운용할 수 있도록 내장형 SW를 설계하여야 한다[2].

[표 1] 무기체계 내장형 SW 상세 분류

구 분		내 용
하드웨어 인터페이스 SW	펌웨어	-
	신호처리 SW	-
내장형 시스템 제어 SW	내장형 운영체제	- 항공기용 실시간 운영체제
	내장형 미들웨어 및 가상 머신	- 실시간, 안전 중시 Java VM - 실시간, 안전 중시 미들웨어 - 센서 기반 감시정찰 소프트웨어 - 무인 전투체계 지원 소프트웨어
	내장형 응용 제어 SW	- 항공기 통합제어 소프트웨어 - 항공기별 계통 장비별 응용 소프트웨어 - 비행 시뮬레이션 및 실시간 훈련 소프트웨어
입출력 서비스 SW	내장형 멀티미디어 응용	-
	내장형 네트워크 응용	-
	양방향 비실시간 내장형 응용	- 개인장비 첨단화 소프트웨어 - 부상자 원격진료 소프트웨어 - 전투훈련지원 소프트웨어
내장형 SW 개발도구	내장형 SW 설계 도구	- 요구사항 관리 소프트웨어 - 형상관리 소프트웨어 - UML 모델링 소프트웨어 - HMI 설계 소프트웨어
	내장형 SW 구현 도구	-
	내장형 SW 검증 및 시험 도구	- 단위시험 소프트웨어 - 정적 분석/검증 소프트웨어 - 항공전자 통합시험 소프트웨어

3. 무기체계 대상 사이버전 동향

3.1 레프트 오브 론치(Left of Launch) 작전

악성코드와 전자기파 등으로 미사일 통제시스템을 교란해 발사 전 시스템을 무력화하는 작전. 미사일 발사를 '준비→발사→상승' 단계로 나눌 때 '발사'보다 왼쪽에 있는 '준비' 단계에서 악성코드나 전자기파 공격으로 시스템을 교란하는 것이다. 그래서 코드명으로 '발사의 왼편'(Left of Launch)이라는 말이 쓰였다. 미국은 2013년 2월 북한의 3차 핵실험 이후에 '레프트 오브 론치' 프로그램을 공개했다. 미국 뉴욕 타임즈는 지난 4월 16일 북한이 발사한 미사일도 발사 직후 곧바로 폭발한 것으로 파악돼 레프트 오브 론치의 결과물일 수 있다고 보도했다[3].

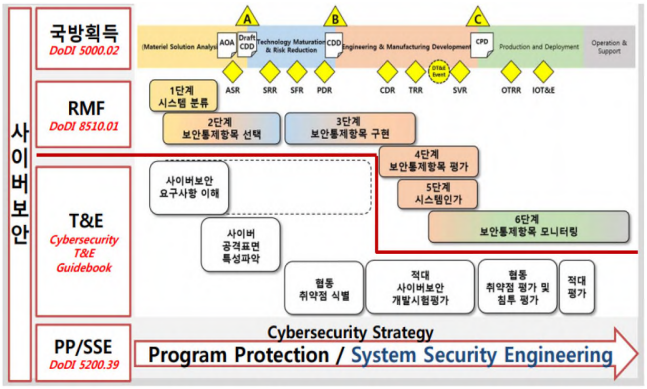
3.2 RQ-170

이란은 RQ-170의 제어 탈취에 교란 및 GPS 탐지 공격을 사용하였다고 주장하고 있으나 일부에서는 이기체가 레이더에 탐지되지 않고 이란의 무인 사막지대에 원인미상의 이유로 고장이 발생하여 불시착 했을것이라고 주장하는 설도 있다. 어떤 경위든 미군의 RQ-170은 이란이 확보하였고 이란은 미 공군도 인정하는 UAV 약점을 제시하고 있다. 이란은 뜻밖의 기회에 세계를 상대로 선전전을 전개하고 자국의 전자사이버 능력의 성과라고 선전하였다. 그뿐 아니라 UAV의 취약점을 분석 제시하며 리버스 엔지니어링을 통해 획득한 정보를 활용하여 신형 전투 무인 항공기 Saeqeh를 개발하여 발표했다[4].

4. 국내외 무기체계의 사이버보안

4.1 미국의 무기체계 사이버보안

미국은 국방부 시스템과 네트워크는 사이버공격에 늘 노출되어 있으며 거의 모든 국방시스템이 어떤 형식이로든 정보기술(IT)을 포함하고 있기 때문에 사이버 적에 대한 회복력을 갖추고 있어야만 한다고 인식하고 이를 위해 무기체계와 플랫폼, 지휘·통제·통신·컴퓨터·정보·감시·정찰(C4ISR)시스템, 그리고 정보시스템과 네트워크 등 모든 분야에 사이버보안을 적용하고 있다. 또한 사이버보안은 국방부의 중요 우선순위로 미국이 기술우위를 유지하는데 필수적이라는 인식下에 일부 정책을 개정하여 획득사업에 사이버보안을 통합하는 것을 보다 강하게 강조함으로써 시스템 회복력을 보장하고자 했다[5].

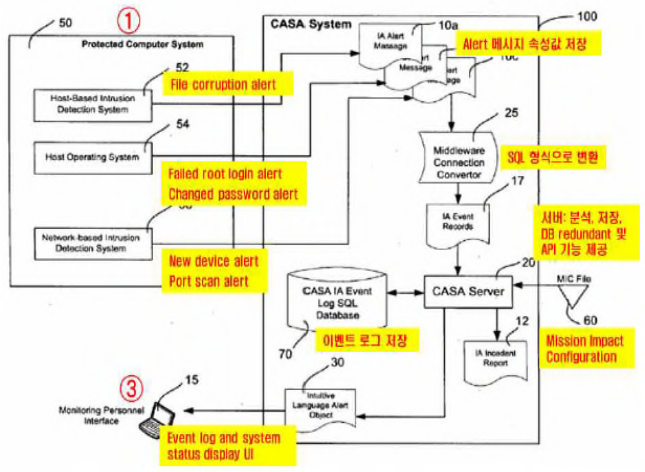


[그림 1] 미국 국방획득체계 사이버보안

이중 사이버보안 시험평가 절차를 살펴보면, [그림 1]에서와 같이 '사이버 시험·평가 가이드북(2015)'에 명시하여 국방획득체계 전 단계에 적용하고 있다. 평가단계는 크게 '개발시험평가'와 '운용시험평가'로 나누어 실시하고 있다. 개발시험평가 단계에서는 설계·구현상 취약점 검증 및 제거, 침투 테스트 등이 이루어지고 있다. 운용시험평가 단계에서는 실제 환경에서의 취약점 확인 및 제거, 사이버 위협에 대한 대응태세 확인 등을 하고 있다. 시험 평가는 Operational Test & Evaluation, Office of the Secretary of Defense에서 담당하고

있으며 매년 발간되는 'Weapons Testing Cybersecurity Report'에 관련내용(시험평가 결과 등)을 수록하고 있다. 또한 개발단계에서의 오류를 최소화 하기 위하여 'Defense Acquisition University'내 무기체계 획득과 정에서 사이버보안에 관한 과목을 교육중에 있다[6].

[그림 2]는 CASA는 美해군 NSWCDD(Naval Surface Warfare Center Dahlgren Division)에 의해 개발된 함정용 정보보호체계로 시스템, 네트워크를 포함한 전체 플랫폼에서 정보보증에 관련된 모든 이벤트를 수집, 분석, 보고하도록 만들어졌다. 전투인원은 CASA가 이벤트를 탐지하여 생성한 경보 메시지를 확인할 수 있으며, 해당 이벤트가 임무에 주는 영향과 수정 방안 등을 확인할 수 있다.



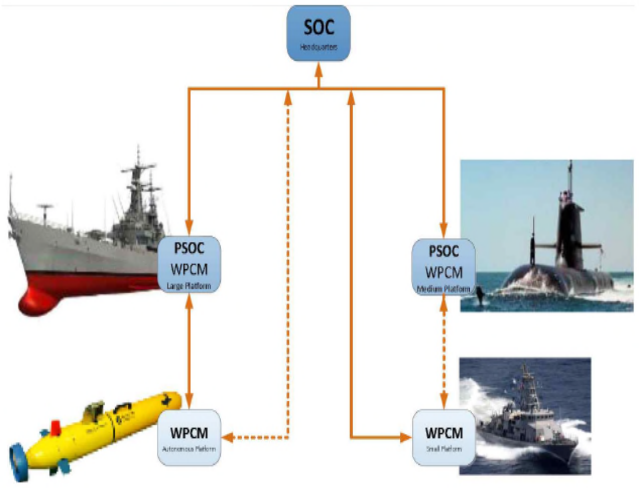
[그림 2] CSCA 시스템 구성도

4.2 이스라엘의 무기체계 사이버보안

Neptune은 이스라엘 IAI ELTA社에서 개발한 함정용 정보보호체계로, 전함, 프리깃함, 잠수함, 무인함 등 해군 플랫폼을 위한 전시 사이버 모니터링 시스템이다. Neptune은 방화벽, 안티바이러스, 네트워크장치, 기타 센서의 이상 상황 이벤트를 취합하여 함정 무기체계 및 부체계의 이상여부를 계층적으로 보고한다. Neptune은 이와같이 여러 소스에서 접수한 사이버 이벤트를 종합하는 솔루션을 제공하며, 해군 지휘부는 Neptune을 이용해 완성된 통합 플랫폼으로의 사이버 뷰 및 함대 사이버 뷰를 제공받을 수 있다.

[그림 3]은 Neptune의 모니터링 및 탐지 레이어는 머신러닝을 사용한 AD(Anomaly Detection : 이상 탐지) 알고리즘과 같은 고급 사이버 탐지 메커니즘을 사용한다. 또한, 이 레이어에서는 전투체계, C4I체계, 정보 체계 등의 플랫폼에서 발생하는 이상 행위를 체계 성능에 영향을 주지 않으면서 기록할 수 있다.

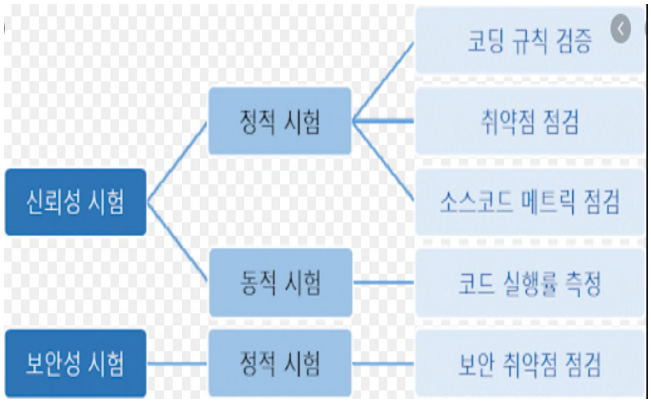
Neptune은 해군 지휘부를 위한 SOC(Security Operational Center, 보안 작전 센터)를 통해 함정 내(onboard) 모니터링 및 해안 원격 사이버 관리를 할 수 있는 기능을 제공한다[7].



[그림 3] Neptune SOC 구조

4.3 한국의 사이버보안 정책

국방부에서는 2013년 신뢰성 시험을 실시하면서 보안성 검증 일부를 실시하기 전까지는 사실상 무기체계 분야는 보안의 대상이 아니었다. 하지만 2017년 6월 국군기무사령부에서 무기체계에 탑재된 'SW 보안성검증' 필요성을 제기하여 국방부에서 국방전력발전업무훈령에 반영, 방사청에서 'SW 보안성 검증' 전면시행을 준비 중에 있다. 무기체계 SW 보안성 검증 시행계획을 살펴보면 '기동·지휘통제·연동 등 무기체계를 구성하는 全SW를 대상으로 검증하는 것으로 되어 있다. 검증절차 또한 체계적으로 잘 정립되어 있다. [그림 4]과 같이 설계 검토 등 문서 검증 2회, 구현 검토를 위한 소스코드 검증 1회를 실시한다는 계획이다. 사업관리부서와 긴밀한 협조를 통해 사업 진행에 영향요소를 최소화 시킬 수 있는 방향으로 시행될 예정이다.



[그림 4] 한국 무기체계 SW 보안성 검증 항목

[그림 5]와 같이 국내 무기체계의 사이버보안으로는 화이트리스트 사이버방호체계는 국방과학연구소에서 개발하여 시범 적용 중인 기술이 다. 실행파일 해시값을 화이트리스트와 비교하여, 미인가 소프트웨어의 실행을 원천적으로 차단할 수 있다. CASA와 유사하게 함정 무기체계의 무결성을 크게 향상시키나, 아직까지 Windows 운영체계만 지원한다. 또한 프로세스 실행 이후 메모리 영역에서의 보호는 다루 지 않는다는 제한점이 있다.

[그림 5] 한국 무기체계 사이버보안

5. 무기체계의 사이버보안 구축 방안

자동화된 위협/방어 에이전트 기술은 현재 선진국에서도 연구개발 초기 단계에 있는 기술로, 다양한 위협/방어 훈련을 통한 사이버전문인력의 전술적 역량을 확보하기 위해 필수적인 기술 중 하나이다. 최근에는 딥러닝 기술 등, 인공지능 기술의 급격한 발달로, 세부적인 시나리오에 의존한 위협/방어 에이전트의 기계적인 위협/방어 수행에서 벗어나, 자유도가 높은, 다양한 사이버 TTP를 수행할 수 있는 기술 개발이 시작되고 있다. 따라서, 이러한 인공지능 기반의 위협/방어 에이전트 기술을 확보한다면 사이버작전 수행을 위한 사이버 전문인력의 전술적 역량 개발에 큰 도움이 될 것으로 기대된다. 복귀 등 사이버 조치과정을 모의하고 기록하여 평가에 반영토록 한다.

현행 사이버 수행, 특히 정보체계용 상에서의 고수준 사이버 대응활동 또는 사이버전문인력에 대한 행위를 분석하고 훈련생 개개인의 역량을 평가하는데 상당한 전문성과 노력이 요구되는 것이 현실이다. 이러한 평가 부담을 덜고 고수준 사이버전 수행의 효과를 크게 높이려면 행위를 자동으로 모니터링하고 평가할 수 있는 빅데이터 모니터링을 통한 AAR 및 자동 평가 기술의 도입이 필수적이다.

6. 결론

국방 분야의 무기체계는 SW에 대한 취약점 점검 및 소프트웨어 개발과정에서 사이버전에 위협에 대응하는 준비가 수행되고 있다. 그러나 미국, 이스라엘에 대비하여 국내 무기체계를 대상으로 하는 보안시스템을 통한 관제 등은 실시되지 못하는 한계를 가지고 있다. 이에 본 논문에서는 해외 무기체계 사이버보안 시스템을 분석하여 국내에도 무기체계에 사이버보안 시스템을 도입하여 사이버전에 대응이 가능하도록 제안하였다.

참고문헌

[1] 최문정, 최준성, 정익래, “무기체계 내장형 소프트웨어 시큐어 코딩 프레임워크”, 한국정보처리학회 2105년 춘계학술발표대회 논문집, 2015

[2] Junesung Choi, “Development of Evaluation Model for Secure Coding Rule Selection Optimized on the System Characteristics”, Seoul National University of Science and Technology

[3] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho Kook, “Defense SW Secure Coding Application Method for Cyberwarfare Focused on the warfare System Embedded SW Application Level”, Journal of Korea Association of Defense Industry Studies, 2012, Vol.19, No. 2, pp. 91-103

[4] 美 RMF 가이드북, pp199

[5] 고려대, ‘사이버보안시험평가를 위한 국방획득체계 RMF 프로세스 적용방안’ 발표자료, 2017

[6] DoDI 8500.01 “Cybersecurity”

[7] DoD Cybersecurity Test&Evaluation Guidebook V1.0