보안공학연구논문지 *Journal of Security Engineering*
Vol.12, No.4 (2015), pp.363-378
http://dx.doi.org/10.14257/jse.2015.08.04

무기체계 임베디드 소프트웨어의 유지보수 체계 개선 및 정보보호체계 구축 방안

박철현[1], 안훈상[2], 김승규[3], 배종호[4]

Strategies to Improve the Management System of Weapon Systems Embedded SW and to Construct its Information Security System

Chulhyun Park[1], Hoon-sang An[2], Seungkyu Kim[3], Jongho Bae[4]

요 약

무기체계 임베디드SW는 그 중요성에 비해 충분한 유지관리가 진행되지 않아 자체 결함 및 외부 침입에 대한 취약성을 내포하고 있다. 이에 따라 현재 관리 실태를 면밀히 관찰하여 군 내 전문인력·조직 구축, 품질보증 제도화, SW ILS 제도화 등 유지보수 체계 개선을 위한 대책을 제시한다. 또한 S-SLA기반 정보보호 유지보수, 화이트리스트 기법 + TPM 적용 등 정보보호체계 구축을 위한 대안을 제시한다.

핵심어 : 무기체계 임베디드SW, SW 유지보수, 정보보호, S-SLA, Whitelist, TPM

Abstract

S. Korea's weapon systems embedded softwares have some vulnerabilities to their own defects and outer invasions as a result of the insufficient maintenance and management system in spite of their growing importance. In this paper, we analyzed the actual outcome of its current operation of management system. Then we introduce a strategy to improve the current maintenance system such as organization of professional maintenance division and institutionalization of SW quality assurance and Integrated Logistics Support(ILS). Lastly, we suggest S-SLA-based security maintenance and Whitelist-based solutions+TPM in order to develop information security system for the weapon systems embedded SWs.

Keywords : Weapon Systems Embedded SW, SW Maintenance, Information Security, S-SLA, Whitelist, TPM

접수일(2015년06월13일), 심사의뢰일(2015년06월14일), 심사완료일(1차:2015년06월30일, 2차:2015년07월15일)
게재확정일(2015년08월05일), 게재일(2015년08월31일)

[1]321-929 충남 계룡시 신도안면 계룡대로 663 사서함 501-8, 육군본부 정보보호/SW정책과
email: kmanp@hanmail.net
[2]321-929 충남 계룡시 신도안면 계룡대로 663 사서함 501-8, 육군본부 정보보호/SW정책과
email: husker@naver.com
[3]321-929 충남 계룡시 신도안면 계룡대로 663 사서함 501-8, 육군본부 정보보호/SW정책과
email: ddoppang@daum.net
[4](교신저자) 305-764 대전광역시 유성구 대학로 99, 충남대학교 정보통계학과
email: bae-jongho@cnu.ac.kr

ISSN: 1738-7531 JSE

1. 서론

북한의 지속적인 안보위협에 따라 군의 무기/비무기체계(전력지원체계)의 첨단화가 이루어지는 현 상황에서 무기체계 소프트웨어(이하 SW)의 유사시 군 주도 유지관리(Maintenance Management) 능력 확보는 필수요소가 되고 있다. 그러나 소스코드를 다룰 수 있는 전문 인력의 부족, 개발 이후 진행되지 않은 임베디드(Embedded) SW 유지보수(Maintenance), 낮은 국산화율과 높은 업체 의존도 등의 현실은 시간이 지날수록 무기체계SW 관리를 어렵게 만들고 있다. 이에 대해서 국방부는 무기체계 임베디드SW에 대한 국산화율을 높이고 수명주기 관리체계 개선을 위한 연구[1], 국방기술품질원은 무기체계 임베디드SW의 획득관리 개선에 대한 연구[2], 방위사업청은 『무기체계SW 개발 및 실무지침서』 등을 통하여 관리개선을 위한 정책 방향을 제시하였으나[3] 육·해·공군에서 직접 적용 가능한 구체적인 대책은 아직 마련되지 않았다.

그리고 2013년 금융업체에 대한 DDoS 공격, 최근 한국 수력원자력 원전자료 유출 사고 등을 계기로 민·관·군 합동 사이버 위기 대응 실전훈련 강화, 사이버 분야 전문 인력 양성 확대, 국가 안보실 중심의 사이버 안보 컨트롤 타워 기능 강화, 2015년 초 합동참모본부 사이버작전과 신설을 통한 군 사이버작전 중앙통제력 강화 등 범국가적인 사이버방호태세가 구축 중에 있다. 그러나 유사시 최고의 성능발휘를 통하여 국가의 안보 일선에서 활용될 무기체계의 임베디드SW는 정보보호체계가 구축되지 않아 자체 결함 또는 외부 침입에 대한 취약성을 드러내고 있다. 이에 대하여 무기/비무기체계 임베디드SW 보안기능 요구사항 분석 및 평가방법의 연구[4], 소프트웨어 보안정책 구현을 위한 무기체계SW 보안성확보 활동 방안[5], 시큐어코딩을 위한 무기체계 임베디드SW 개발보안 적용분류체계[6] 등의 연구가 꾸준히 진행되었다. 그러나 여전히 무기체계 임베디드SW에 적용 가능한 중·장기적인 발전 방향과 현실적 대안 및 구체적 활동 계획의 수립이 절실한 시점이다. 따라서 본 논문에서는 무기체계 임베디드SW의 현재 관리 실태와 정보보호의 현실을 살펴보고 그 특성에 부합하는 대안을 제시하고자 한다. 이를 통하여 우리 군이 보유한 무기체계 임베디드SW의 원활한 유지보수 체계를 정착시키고 현실적인 예산 환경 하에서 효율적인 정보보호의 추진에 기여하기를 기대한다.

2. 무기체계 임베디드SW의 현 실태 분석

2.1 유지관리 실태

국방SW는 무기체계SW와 전력지원체계SW로 구분 되며, 무기체계SW는 다시 전장관리체계SW와 무기체계 임베디드SW로 구분된다([그림 1] 참조). 전장관리체계SW는 주로 유사시 지휘통제·전투지휘·군사정보체계 정보의 수집·가공·저장·검색·송/수신 및 활용에 관련된 SW로서 합동지휘통제시스템(KJCCS : Korea Joint Command and Control System), 육군 전술지휘정보체계(ATCIS: Army

Tactical Command Information System), 해군 전술C4I시스템(KNCCS : Korea Naval Command and Control System), 공군 전술C4I시스템(AFCCS : Air Force Command and Control System) SW가 포함된다. 무기체계 임베디드SW는 무기체계에 내장되어 임무수행에 전용으로 제공되는 SW로서 감시/정찰·항공·화력·방호·기동 무기체계용 SW를 포함한다. '무기체계'의 범주에서 전장관리체계SW와 임베디드SW 간에 기술적인 큰 차이는 없으나 전장관리체계SW는 임베디드의 성질과 비(非)임베디드 성질의 SW를 두루 포함하는 특성이 있다. 무엇보다 가장 큰 차이는 전장관리체계SW는 국산화율이 비교적 높고 관리조직이 편성되어 있는 반면, 무기체계 임베디드SW는 외산 의존도가 더 높고 군에 관리조직이 아직 편성되지 않았으며 정보보호 대책이 수립되지 않았다.

[그림 1] 국방SW 분류[1]

[Fig. 1] Classification of the National Defense SW

2.1.1 인력 운영적 측면

무기체계는 지금도 여러 체계들이 지속적으로 개발 중이므로 현재의 조직과 인력으로는 유사시 원활한 운영유지가 제한된다. 또한 군이 핵심기술을 모두 보유하고 있지 않기 때문에 유사시 소스코드를 핸들링 하는 성능개량에 한계가 있다. 즉, 소규모 오류제거는 가능하지만 변경소요가 큰 성능개량은 제한된다. 위 문제들을 보완하기 위해서 최초 개발에 참여했던 전문 인력들을 유사시 어떻게 확보할지 구체적인 계획이 요구된다.

2.1.2 제도/조직적 측면

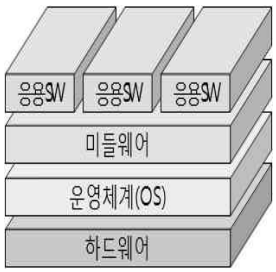
무기체계의 하드웨어(이하 HW)부분은 종합군수지원(ILS : Integrated Logistics Support)상에 정비계획을 구체화하도록 제도화 되어 있으나, 상대적으로 중요성이 덜 부각되는 SW 정비계획은 누

락되거나 반영되지 않는 경우가 많다. 특히, 유사시 동원되는 기술인력은 주로 HW와 상용SW 정비를 위한 인원으로서 개발된 SW를 유지보수하기 위한 전문인력 동원계획은 정립되지 않았다. 또한 무기체계 임베디드SW의 경우 전장관리체계SW와는 달리 각 군의 개발 이후 유지보수 - 재개발 - 폐기 관리를 위한 조직 구축이 미흡하고 개발 이후 SW에 대한 유지보수는 진행되지 않았다. 주된 이유는 최초 개발 시 장비 및 HW 위주로 정비계획을 수립하여 SW 유지보수에 대한 책임부서가 정해지지 않았기 때문이다. 따라서 무기체계 임베디드SW의 유지보수 및 수명주기 관리를 위한 임무·교리/교육·제도/조직·인력·환경·예산 등을 포함하는 계획 작성이 시급한 실정이다. 이에 대해 국방부는 보고자료 『무기체계 임베디드SW에 대한 국산화 향상 및 관리체계 개선방안』 [1]을 발표하여 해결책을 모색 중이나 세부적인 대응계획과 각 군의 역할은 아직 정립되지 않았다.

2.1.3 환경적 측면

무기체계SW의 중요성 인식의 확산과 더불어 유지관리를 위한 기반 환경 조성이 선행되어야 하나 현재는 매우 열악한 상황이다. 무기체계 임베디드SW는 개발 전부터 SW 유지보수가 고려되지 않았기 때문에 군 자체 유지보수를 위한 테스트베드, 시험장비(시뮬레이터 등), 코딩 검증 및 재사용성을 위한 툴·시설 등 기반여건이 전혀 구축되지 않았다.

2.1.4 기술적 측면



응용SW	특정한 기능을 수행하도록 만들어진 응용 프로그램 (예: 한글, 자동제어, 지휘통제, 비행제어, 사격통제 등)
미들웨어	응용SW와 운영체계(OS) 사이에서 매개역할을 하는 중간 프로그램 (예: DBMS, 통신미들웨어(RTI) 등)
운영체계 (OS)	컴퓨터를 작동시키고 응용SW가 효율적으로 실행될 수 있는 환경을 제공하는 기본 프로그램 (예: Window XP, Linux, VxWorks 등)

[그림 2] 무기체계SW 세부 계층[7]

[Fig. 2] Stratification of Weapon Systems Embedded SW

북한의 지속적인 안보위협에 따라 군의 전시(戰時) 정보체계인 전장관리체계의 기술도 첨단화가 이루어지는 현 상황에서 전장관리체계·내장형SW를 포함하는 무기체계SW의 유사시 군 주도 유지관리 능력 확보는 필수요소가 되고 있다. 특히 유사시는 평시보다 외주업체 지원을 받는 것이 제한되므로 군 주도적인 SW 유지관리가 불가피하다. 미군의 경우 국방부 자체 유지보수를 통한 유사시 SW유지관리의 효율성을 강조한 바 있다[8]. 그러나 무기체계 임베디드SW 핵심기술의 업체 의존도는 심화되어 있고 운영체계·미들웨어·응용SW([그림 2] 참조) 모두 외산 의존도가 높지만 유사시 관리지원 가능한 업체의 동원이나 군 주도 유지관리를 위한 계획이 수립되지 않았다. [표 1]과 같은 임베디드SW의 특성은 다른 SW보다 더 전문적이고 업체의존도가 심화된 이유를 말 해 준

다. 특히 '고신뢰성'은 한 건의 오류가 치명적 인명피해를 초래할 수 있는 무기체계 임베디드SW의 대표적 특성으로서 오류 최소화를 위한 신뢰성 시험과 품질관리 테스팅의 제도화 역시 시급함을 유추할 수 있다.

[표 1] 무기체계 임베디드SW의 특성[7]
[Table 1] Characteristics of Weapon Systems Embedded SW

• 실시간성 : 무기체계 성능발휘를 위해 주어진 시간 내 이벤트 처리 요구 • 시험난이성 : 체계별 상이한 SW 내장으로 상호호환 제한 • 고신뢰성 : 불안정한 전장환경 속 운용을 위한 고도의 신뢰도/가용도 요구 • 목적 한정성 : 특정 무기체계 임무목적에 따른 개발 • 개발 난이성 : HW에 따라 개발언어·관련지식이 상이하며 호스트(host)와 타깃(target)으로 구성된 교차개발 환경을 모두 고려하여 개발 • 하드웨어 통합성 : HW와 동시설계·개발되므로 HW·SW 통합 가능한 전문지식 요구

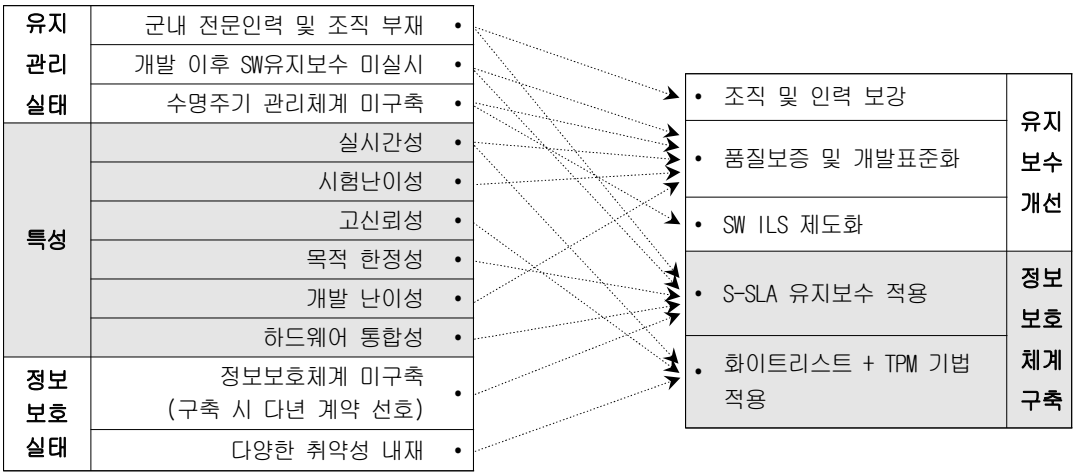
2.2 정보보호 실태

전술한 바와 같이 무기체계 임베디드SW의 경우 SW에 대한 유지보수가 진행되지 않고 있으며, 이에 따라 현재 배치되어 운용 중인 체계들 중 공군의 항공 관련 일부 체계를 제외하고 대부분 오류 수정·신뢰성 보장 및 정보보호 활동이 진행되지 않았다. 특히 무기체계 SW 개발과정에서 SW 자체 취약점으로 인한 침해 사고를 최소화하기 위해서 가장 현실적인 대안이 될 수 있는 SW개발 보안(시큐어코딩)[9] 역시 적용되지 않았다. 특히 시큐어코딩의 미적용 상태에서 적응 유지보수가 되지 않아 SW의 복잡도가 증가하는 경우, 'SW의 복잡도는 보안의 적'[10]이라는 말처럼 보안에 취약해 질 수밖에 없다. 임베디드SW의 경우 소프트웨어 변조·소프트웨어 구현·하드웨어 외부·하드웨어 터미널·하드웨어 컴포넌트 침입·하드웨어 복제·데이터·시각정보·사용자 인터페이스·시스템 접근·암호구현으로 구분되는 카테고리 안에 59개의 취약성 요소를 포함하는 연구결과가 보고되었다[3]. 실제로 시스템에 대한 전력분석공격(power analysis attack), 오류주입 공격(fault attack), 전자기 공격, 그리고 칩 디캡핑(chip de-capping), 마이크로프로빙(micro-probing) 등 물리적 공격의 사례들이 보고된 바 있다[3]. 유사시 인명손실과 직결된 무기체계의 고신뢰성 측면에서 볼 때 자체 내포된 결함이 식별되지 않고 있거나 외부침입에 대한 대책이 수립되지 않았다는 점은 조속한 조치가 필요한 부분이다.

3. 개선 전략 도출

무기체계 임베디드SW의 현 실태를 극복하고자 2014년 7월부터 2015년 2월까지 육·해·공군 정보화기획실 중심으로 각 군 및 방위사업청 SW개발자·운영 실무자, 정보보호 담당자, 국방기술품질원 담당자들이 총 5차례의 실무토의와 연구보고를 통하여 개선 전략을 도출하였다. 즉, [그림 3]과 같

이 현재 유지관리 실태와 무기체계 임베디드SW의 특성, 그리고 정보보호 실태를 교차 분석하여 유지보수 개선을 위한 과제로서 '조직 및 인력 보강', '품질보증 및 개발표준화', 'SW ILS 제도화'를 도출하였으며, 정보보호체계 구축을 위한 과제로서 'S-SLA 적용', '화이트리스트+TPM 기법 적용'을 도출하였다. 도출된 이유와 추진 방향의 자세한 내용은 아래 절에서 이어서 설명하겠다.



[그림 3] 무기체계 임베디드SW 개선 전략 도출

[Fig. 3] Improvement Strategies Derived for Weapon Systems Embedded SW

3.1 유지보수 개선 방안 도출

수명주기 관리가 미흡한 무기체계 임베디드SW의 관리 실태와 실시간성·시험난이성 등 고유의 특성을 분석하여 우리가 해야 할 일을 아래와 같이 도출하였다.

첫째, 조직 및 인력 보강이다. 무엇보다 수명주기관리 전담조직을 국방부와 각 군에 신설해야 하며 그에 따라 교리/교육·제도/조직·인력·예산·관리대상 등 세부계획을 지금부터 작성해야 한다. 또한 SW개발에 참여한 기술 인력의 명단을 확보하고 유사시 원활한 SW 유지보수·성능개량이 이루어질 수 있도록 동원계획에 반영해야 한다. 특히 그 동안 관리되지 않은 SW 수량이 방대한 만큼 전투 긴요도와 개발비용이 높고 군이 기술소유권(기술소유권 또는 실시권이 없으면 소스코드 핸들링에 제약이 있다.)을 보유한 SW부터 우선 관리대상으로 선정하여 차근차근 관리 규모를 확대해야 하겠다. 또한 기술소유권을 미확보한 체계는 유사시 중단 없는 유지보수가 가능하도록 유지보수 업체와 사전 계약을 체결해야 한다.

둘째, 품질보증 및 개발 표준화를 위한 로드맵을 작성해야 한다. 무기체계 특성 상 SW신뢰성[11]을 확보하고 적시 지원성 향상을 위한 제도 개선이 시급하다. 유형적인 장비·HW 분야는 이미 2014년 초부터 RAM(Reliability·Availability·Maintainability : 신뢰도·가용도·정비도) 분석을 의무화하여 신뢰성 증대의 노력을 강화하고 있으므로 SW 분야도 이에 신속하게 대응해야 한다. 예를 들

어, SW의 신뢰성 목표값(목표 신뢰도)[12]을 설정하고 수명주기 전 단계에 정적·동적 시험을 포함한 SW 테스팅을 제도화하는 등 지속적인 신뢰성 및 품질관리가 필요하다. 이와 관련하여 SW의 잠재된 결함(오류)이 수명주기 전 단계에서 불규칙적으로 생성되는, 즉, 비동차 포아송과정(NHPP: Non-Homogeneous Poisson Process)을 따르는 모형에 대한 연구[13], 개발단계에서의 SW신뢰성[14], 운영단계에서의 SW신뢰성[15] 관리에 대하여 연구된 바 있다. 또한, 국방SW통합관리체계(DESIS)(DEfense Software Information System : 무기체계 임베디드SW의 사업관리·품질보증 및 저작권 관리를 위해 국방기술품질원에서 개발하였으며 C언어·JAVA·Ada 계열로 개발되는 SW에 적용 가능한 툴)와 같은 전문적 관리 툴을 활용하여 잠재성 오류 분석·복잡도 분석·유지보수성 분석 등 품질보증을 위한 활동이 강화되어야 한다. 더불어, 개발된 체계 간 상호운용성·재사용성[16][17] 증대를 위한 개발방법론 등 표준화 향상을 위한 제도 개선이 절실하다.

셋째, 군 자체 유지보수 및 성능개량을 위한 기반체계 구축이다. 즉, 유형적인 HW 위주로 작성되는 종합군수지원(ILS)에 SW 유지보수 항목을 명시하고 준수하도록 제도화해야 하며([표 2] 참조), 개발 전부터 테스트베드 및 시험장비(시뮬레이터 등) 확보를 위한 예산을 반영하여 전·평시 간단없는 결함 식별 및 보완, 신뢰성 유지를 위한 SW 테스팅 등이 이루어지도록 추진해야 한다.

[표 2] SW에 대한 ILS 요소 (예시)[1]
[Table 2] An Example of ILS Factors for SW

ILS 요소	세부사항
연구/설계 반영	· SW ILS 요소 및 요구사항을 설계에 반영 · SW 유지보수 지원체계를 고려하여 설계
표준화/호환성	· SW 표준화 및 유사체계와 호환성 · 표준 준수 여부 및 상호운용성 검토
정비계획	· SW 정비지원을 위한 지원요소 분석/개발 · 소요군 정비능력 확보
지원장비	· 정비단계별 유지보수에 필요한 소프트웨어 확보 · SW 정비결과 확인을 위한 시뮬레이터 개발
군수인력운용	· 정비요원, 기술수준에 맞는 인력 충원 · 소요 주특기 판단
군수지원교육	· SW 운용자 교육계획 · 교재/교보재 지원, 체계 소개용 동영상 제작 등
기술교범	· SW 설치 매뉴얼, 소프트웨어 버전기술서 · 소프트웨어 사용자 및 운용자 설명서
기술자료관리	· 소프트웨어 산출물, 체계개발 설계, 구현, 시험관련 자료, 응용 소프트웨어 소스코드 등

3.2. 정보보호체계 구축

3.2.1 S-SLA 유지보수 적용

현재 무기체계 임베디드SW를 제외한 전장관리체계 또는 비무기체계(전력지원체계)의 경우 정보보호 솔루션이 대부분 민간 용역 유지보수로 진행되고 있다. 특히 HW와 결합된 접근통제/침입차단시스템·백신 등은 5~6년 단위 리스 계약과 요율제 유지보수[18]를 병행하고 있으며 보호체계 도입 시 공통평가기준(CC : Common Criteria) 인증을 의무화하고 있다. 그러나 무기체계 임베디드SW의 경우 개발시 시큐어코딩과 정상적인 유지보수가 진행되지 않으며 다양한 개발언어와 기능, HW별 플랫폼이 상이한 특성을 가지고 있기 때문에 기존과 다른 유지보수 방식이 요구된다. 즉, 일반적인 요율제 유지보수보다는 성과중심의 유지보수로 보호수준 강화 과정이 가시화 및 통제되어야 하며, 보호체계의 미도입에 따라 CC인증 수준의 보호 대책이 요구된다. 이에 대하여 S-SLA(Security-Service Level Agreement), 즉, 보안 서비스 수준에 따른 계약방법을 대안으로 고려할 수 있다.

SLA는 보장된 품질 수준에 관련된 측정지표를 기술하는 서비스 제공자와 사용자들 사이의 공식적인 계약이다. 일반적인 SLA는 대역폭, 지연, 손실 등과 같은 유지보수에 관련된 측정지표와 보장수준을 나타낸다[19]. 서비스 제공자에 의하여 구현되는 SLA는 측정 및 추적될 수 있는 지표에 기초한다. 이와 같은 측정지표로 서비스 제공자 뿐만 아니라 사용자들도 잘 이해하고 있는 서비스 가용성(availability)을 예로 들수 있다. 예를 들어, 특정 보안서비스의 가용도가 99.999%일 때 1년에 접속 불량 시간 10분 이내의 품질 서비스 제공이 가능하다는 의미를 가지고 있다[19]. 즉, 일반적으로 요율제 유지보수는 계약기간 동안 예상되는 결함 수정이나 기능개선의 분량을 대략적으로 산정하여 계약 시 선급금으로 50% 이상 지급하고 만료 시 잔금을 지급하는 형태가 대다수로서 성과에 대한 평가는 미약한 편이다. 반면, SLA 유지보수는 용역업체가 관리해야 할 영역을 식별하여 목표값을 산정한 후 서비스 수준과 성과지표로 제시하고, 목표 미달 시에는 제재(penalty)를, 성과가 만족스러운 경우는 보상(incentive)을 제공한다. 이는 성과기반 관리방식에 있어 보다 체계적인 군수 분야에서의 PBL(Performance Based Logistics : 성과기반 군수관리제도)과 유사하다. PBL은 용역업체에 군수지원요소의 성과목표/성과지표를 제시하고 군수공급관리체계의 책임을 업체에 위임함으로써 군으로 하여금 본연의 임무에 집중하도록 하며, 재고비용 감소, 공급체계 효율성 증진, 저 신뢰도 부품에 대한 성능 및 가용성 개선을 통한 비용을 절감하는데 그 목표가 있고 성과목표 유지에 대한 인센티브를 제공한다[20]. 즉, S-SLA와 PBL 방식은 군이 더욱 전투에 전념하고 유지보수 및 정보보호는 민간에 위탁하여 효율성을 높이고 비용을 줄이려는 공통적인 목표를 갖는다.

무엇보다 시큐어코딩과 SW 유지보수가 진행되지 않은 현 상황에서 전문업체에 의해 보안수준을 진단하고 요구 수준을 달성하여 효율적으로 유지하기 위한 성과 위주 관리체계가 필요하다. 여기서 공통 플랫폼이 정립되지 않고 HW에 따라 기능과 언어가 상이한 무기체계 임베디드SW의 현실은 체계별 상이한 보안기능을 요구하므로 서비스 수준과 성과지표가 적절히 등급화 되어야 한다. 또한, 다음 년도 성과지표를 작성하기 위해서는 이번 년도 성과가 필요하므로 일반적인 요율제 유지보수처럼 1년 단위 계약방식보다 다년 단위 계약 방식이 적절하다.

서비스 수준과 성과지표를 결정하기 위한 보안기능 요구사항은 국가보안기술연구소에 의해 통신 채널 보호·데이터 보호·암호지원·시스템 접근 보호·물리적 보안·시스템 자체보호·보안감사·구현 안전성·성능 및 가용성의 9가지 카테고리로 구분하여 제시되었으며[3], 또한 S-SLA 성과지표의 등급화를 침입탐지 시스템과 안티바이러스 시스템에 각각 적용한 연구가 진행된 바 있다[19][21]. 즉, 각각의 체계 특성에 부합하는 적절한 보안기능 요구사항을 선택하고 등급화 하여 서비스 수준으로 제시할 수 있다. 등급화는 공통적인 보안기능일수록 하위 등급으로 분류하고 개별적인 기능일수록 상위 등급으로 분류할 수 있는데[19][21], 무기체계 임베디드SW는 아직 정보보호 관련 유지보수 실적이 없으므로 최소 1년 이상 유지보수를 진행한 후 그 결과를 바탕으로 S-SLA를 위한 등급화 지표를 개발하는 것이 타당하겠다. [표 3]은 서비스 수준을 정의하기 위한 보안기능 요구사항의 예시이다. 여기서 A등급은 B등급보다 체계에 공통적으로 적용되는 보안기능이다.

[표 3] 보안기능 요구사항 예시
[Table 3] An Example of Security Function Requirements

체계/언어	기능	보안기능 요구사항	등급수준
감시 정찰 체계 / C ++	보안감사	보안감사 데이터 생성	A
		보안감사 데이터 접근 통제	
		보안감사 데이터 무결성	
		보안감사 데이터 저장	
	시스템 접근보호	관리자 및 시스템 권한 명세	A
		관리자 식별 및 인증	
		연속 인증 실패	
		사용자 권한 명세	
		사용자 식별 및 인증	
		세션 잠금 및 종료	B
	:	:	:

3.2.2 화이트리스트+TPM 기법 적용

무기체계 임베디드SW의 실시간성 특성 상 무기체계가 주어진 시간 내 이벤트를 처리하고 성능 발휘를 하기 위해서 복잡도가 크고 부담스러운 안티바이러스 솔루션은 장애가 될 수 있다. 반면 다양한 정보보호 취약성을 내포하고 있기 때문에 알려지지 않은 다양한 침해에 대응 가능한 대책이 필요하다. 더불어 무기체계 임베디드SW의 시험 난이성과 목적 한정성의 측면에서 볼 때 특정 영역에 제한된 업무처리, 폐쇄 또는 단독망 형태, 리소스가 많지 않고 전장관리체계에 비해 저사양이라는 특성은 기존의 방역체계인 블랙리스트 기법과 차별되는 대안을 요구한다. 따라서 알려진,

또는 알려지지 않는 악성코드 침해에 대해 아래와 같이 화이트리스트 기법을 적용한 관리체계를 대안으로 고려할 수 있다.

[표 4], [표 5]에서 알 수 있듯이 다수의 안티바이러스 솔루션을 포함하는 블랙리스트 기법은 위험성이 입증된 악성코드에 대해서만 유입을 차단하지만 전장관리체계SW에 비해 운영범위가 작은 임베디드SW는 특정 허용된 실행(executable)파일을 제외하고 모두 차단시키는 방법을 적용하는 것이 효과적이다[22].

[표 4] 화이트리스트 vs 블랙리스트 기법 비교[22]
[Table 4] Comparison of Whitelist Solutions vs. Blacklist Solutions

구 분	화이트리스트 기법	블랙리스트 기법
처리방식	사전예방	사후처리
프로그램제어	허용된 어플리케이션만 사용	모든 어플리케이션 사용 가능
편의성	제한적 환경	범용적 환경
엔진 사이즈	변경없음	지속적인 증가
리소스 점유율	낮음	높음
보안수준	높음	낮음
업데이트/패치	업데이트가 필요한 경우 정기적인 라인 점검 시 스케줄링 가능	실시간 업데이트/패치 적용으로 장애 발생 우려

[표 5] 화이트리스트 기법 특성[22]
[Table 5] Characteristics of Whitelist-Based Solutions

- 안전한 것으로 증명된 입력값만 허용, 증명되지 않는 신종 악성 코드 차단 및 Zero-Day Attack까지 진단 가능
- 특정 프로그램만 사용되는 제한적인 환경에 적합
- 변화가 적고 운용 프로그램 수가 적은 산업용 기기에 적합
- 초기 코드 내 악성코드 내포 시 화이트리스트로 인식될 수 있으므로 시스템의 무결성 보장 필요

화이트리스트 기법은 일반적으로 응용프로그램(어플리케이션)을 구성요소로 식별하여 화이트리스팅 정책과 결합시키는 몇 가지 공통된 방법에 기초를 두고 있으며, 이는 인증서(certificate), 경로값(path values), 해시값(hash values), 서비스(service) 그리고 시스템 및 사용자 요소(system and user behavior) 등을 포함한다[23]. 화이트리스트를 활용한 악성코드 설치를 위해 악용되는 웹사이트 탐지에 관한 연구[24], 제어시스템을 대상으로 하는 고도화된 사이버 공격과 다양한 오작동 상황에 대처하기 위해 화이트리스트 기반으로 이상 징후를 탐지하는 연구[25], SW 업데이트 유형별 위협요소와 그에 대한 안전성 강화를 위한 화이트리스트 구성방안에 대한 연구[26] 등이 진행된 바 있다. 단, 화이트리스트 기법이 블랙리스트보다 초기 비용소요가 크기 때문에 도입에 장애요소

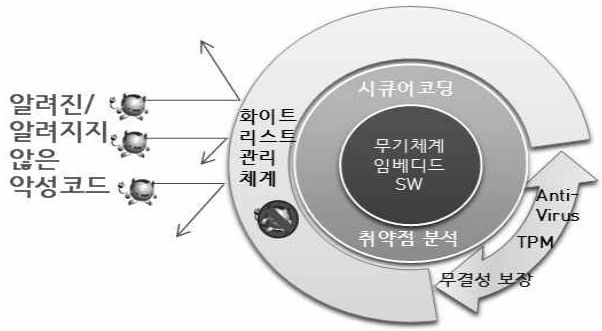
가 될 수 있으나[22] 이는 차후 SLA에 의한 협약과 수명주기 비용분석을 통하여 적절한 소요비용을 산정해야 할 문제이다.

또한 화이트리스트 기법의 특성에서 알 수 있듯이 화이트리스트를 적용하기 위해서 사전 시스템의 무결성이 보장되거나 지능적으로 악성코드를 제외한 후 화이트리스트를 작성할 수 있는 기술력이 요구된다[22]. 이에 대해 TCG(Trusted Computing Group)의 TPM(Trusted Platform Module)이나 안티바이러스 솔루션을 병행 사용하여 이를 보완하는 방법을 고려할 수 있다. 안티바이러스 솔루션이나 기타 보안프로그램은 운영체제가 안전하다는 전제조건 하에서 사용되는데, 운영체제나 SW의 취약점을 이용한 Zero-Day Attack이 발생하는 경우에 대비하여 HW단계에서 차단하는 TPM 기법이 제기되었다[27]. TPM 기법은 HW 단계에서 자료를 암호화 및 복호화 할 수 있도록 하여, 디스크만 추출해서 내부 자료를 탈취하려는 시도 역시 차단가능하다. [표 6]은 이러한 TPM 기법의 특성을 보여준다.

[표 6] TPM 특성[22][27][28]
[Table 6] Characteristics of TPM

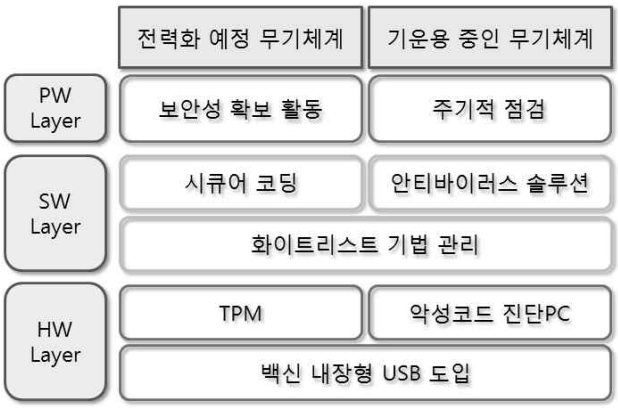
• Zero-Day Attack 등 알려지지 않는 공격을 HW 단계에서 차단 가능한 칩 형태의 모듈 • 암호키 생성 및 암호화 과정을 수행하여 필요한 정보를 보호 • 암호키나 패스워드를 비휘발성 공간에 저장하고 저장 공간에 접근할 수 있는 명령어 제공 • 원격 호스트의 무결성 검증, 신뢰성 기반 통신, 안전한 통신 채널 제공 등 신뢰성 컴퓨팅 플랫폼으로서의 기능 수행

무기체계 임베디드SW처럼 제한된 리소스의 무선 센서 네트워크 상에서 TPM 기법을 이용한 정보보호 및 프라이버시 매커니즘 구축[28], TPM 기법을 활용하여 네트워크 스토리지 환경에서 서버가 클라이언트 호스트의 플랫폼을 인증하는 방법[27]과 프로그램 카운터 인코딩을 구현하는 방법[29] 등은 연구된 바 있다. [그림 4]는 화이트리스트 기법의 관리체계를 TPM 등으로 보완하는 방역체계를 나타낸다.



[그림 4] 무기체계 임베디드SW에 대한 화이트리스트+TPM
[Fig. 4] Application of Whitelist+TPM Solutions to Weapon Systems Embedded SW

정리하면, 가장 이상적인 정보보호체계는 개발 시 시큐어코딩이 적용되고 HW단계에서 TPM이나 SW단계에서 안티바이러스 솔루션을 적용하여 무결성이 보장된 후 화이트리스트를 적용하여 보안체계를 강화하는 것이다. 단, 일부 운용중인 체계 중 유지보수가 진행되지 않아서 초기상태의 BIOS를 유지하고 있는 경우 섣불리 TPM을 새로 장착하기보다 악성코드 진단PC를 설치하여 대처해야 한다는 의견이 있다. 또한 폐쇄망·단독망으로 구성되는 무기체계 임베디드SW의 특성에 따라 망 to 망 연결 시 주로 사용되는 USB 드라이브에 백신을 내장하여 무결성을 강화하자는 의견도 있다. 더불어 시큐어코딩이 미적용 되었기 때문에 SW단계에서 안티바이러스 솔루션으로 악성코드를 식별하고 삭제할 때 시스템 작동 오류가 예상된다면 default로 재셋팅하는 방법도 고려해야 한다. 따라서 아래 [그림 5]와 같이 전력화 예정이거나 신규개발 체계의 경우 시큐어코딩 ⇒ BIOS 또는 시스템 호스트에서 TPM으로 기기의 무결성 확보 ⇒ 화이트리스트 기법을 적용할 수 있으며, 기운용 중인 SW 중 TPM 적용이 제한되는 경우 악성코드 진단 PC 설치 ⇒ 안티바이러스 솔루션 및 화이트리스트 기법을 적용하여 정보보호체계를 구축하는 것이 바람직하겠다.



[그림 5] 무기체계 임베디드SW의 정보보호체계 구축을 위한 층화

[Fig. 5] Stratification for Construction of Security System of Weapon Systems Embedded SW

4. 결론

첨단과학의 발달은 무기체계 기술의 급속한 발전을 초래하였으며 그에 따라 무기체계에 탑재된 SW의 비중은 더욱 커지고 있다. 그러나 그 중요성에 비해 무기체계 임베디드SW는 충분한 유지관리가 이루어지지 않았다. 특히 현재 운용되고 있는 체계는 공군을 제외하고 거의 SW에 집중된 유지보수가 진행되지 않았으며 정보보호 대책도 수립되지 않았다. 이에 따라 본 논문에서는 무기체계 임베디드SW의 관리 실태를 면밀히 관찰하고 그에 대한 대책으로서, 군내 전문인력을 확보와 유지보수 및 관리를 위한 전담조직을 각 군에 신설, 무기체계 임베디드SW의 고신뢰성 등의 특성을 고려하여 적합한 품질보증 제도 및 개발표준화 추진, 그리고 SW ILS를 제도화하여 개발 단계

부터 체계적으로 관리할 것을 제안하였다.

또한, 무기체계 임베디드SW의 정보보호체계 구축을 위한 방안으로서, 성과기반의 정보보호 수준을 유지 및 보안 품질관리 중심의 수명주기 비용 절감을 위한 S-SLA 기반의 정보보호 유지보수 적용, 블랙리스트 기법보다는 화이트리스트 기법+TPM(또는 안티바이러스 솔루션 등)을 적용하여 무기체계 임베디드SW 특성에 맞는 정보보호 체계를 구축할 것을 제안하였다.

향후에는 제시한 대안들을 적용한 결과를 바탕으로 보완 발전된 연구와 블랙리스트 기법과 화이트리스트 기법의 수명주기 비용 비교 및 최적화에 대해 연구하고자 한다.

References

[1] S. Korea's Ministry of National Defense, Strategies to Enhance Localization and to Improve Management Systems of Weapon Systems Embedded SW **(2014)**.

[2] K. Y. Kwon and K. H. Kim, A Study on Importance of the Aquisition Management for Weapon Systems Embedded Softwares, Defense Agency for Technology and Quality, Seoul, Korea **(2001)**.

[3] S. Korea's Defense Acquisition Program Administration, A Handbook on the Development and Management for Weapon Systems SW **(2013)**.

[4] S. Korea's National Security Research Institute, Security Policies and Evaluation Methods for Weapon & Non-weapon systems, supported by Ministry of National Defense **(2011)**.

[5] Ki-Young Lee, Activity plan of guaranteing Software Security of Weapon system for realizing Software Security Policy, Journal of SERSC **(2015)**, Vol.12, No.2, pp.131-138.

[6] Junesung Choi and Kwangho Kook, Developing Warfare System SW Development Security Classification System Using KJ method, Journal of SERSC **(2014)**, Vol.11, No.2, pp.165-176.

[7] S. Korea's Defense Agency for Technology and Quality, 2010 Defense Technical Investigation Paper **(2010)**.

[8] Hagen Christian and Sorneson Jeff, Delivering Military Software Affordably, Defense AT&L: March-April **(2013)**.

[9] Junesung Choi, Wooje Kim, Wonhyung Park and Kwangho Kook, Naval Combat Management System Secure Coding Rule Selection Using Warfare System SW Secure Coding Rule Evaluation Model, Journal of SERSC **(2013)**, Vol.10, No.4, pp.417-428.

[10] B. Schneier, Crypto-Gram Newsletter **(2000)**.

[11] C. V. Ramamoorthy and F. B. Bastani, Software reliability - Status and perspectives, IEEE Trans, on Software Eng. **(1982)**, Vol. SE-8.

[12] Lyu, Michael R., Software Reliability Engineering: A Roadmap, ICSE **(2007)**.

[13] H. Ascher and H. Feigold, Repairable Systems Reliability: Modeling, Inference, Misconceptions, and Their Causes, Marcel Dekker **(1984)**.

[14] Gye-Tak Yang, A Study on the Reliability of S/W during the Developing Stage, Journal of KSIIS **(2009)**, Vol.14, No.5, pp.61-73.

[15] Gye-Shik Che, A Study on the Software Reliabliliy of Operational Stage S/W, Journal of KIMICS **(2008)**, Vol.13, No.3, pp.445-450.

[16] P. Freeman, A Perspective on Reusability, Tutorial : Software Usability, IEEE **(1987)**.

[17] M. D. Mclloy, Mass Producted Software Component, Software Engineering, Naur and Randell(eds.) **(1967)**.

[18] Korea Software Industry Association, A Guide for Calculating Cost of SW Projects **(2014)**.

[19] Wansuk Yi, Woong Go, Dongho Won and Jin Kwak, Development of S-SLA's Grading Indicator based on the Analyses of IPS's Security Functions, Journal of KIISC **(2010)**, Vol.20, No.6, pp.221-235.

[20] H. J. Han and H. S. Moon, Understanding and appling methods of PBL for the ROK military, Defense Technology, Apl **(2009)**, pp.89-97.

[21] Wan-Suck Yi, Dongbum Lee, Dongho Won and Jin Kwak, Development of S-SLA based on the Analyses of Security Functions for Anti-virus System, Journal of KIISC **(2010)**, Vol.20, No.6, pp.237-249.

[22] Whitelist Security, Network Times **(2010)**, pp.153-162.

[23] Dave S., Application Whitelisting: Enhancing Host Security, A SANS Whitepaper **(2009)**, pp.1-14.

[24] Jung Woo Ha, Huy Kang Kim and Jong-in Lim, Reseach on Malicious Code Hidden Website Detection Method through WhiteList-based Malicious Code Behavior Analysis, Journal of KIISC **(2011)**, Vol.21, No.4, pp.61-75.

[25] Hyunguk Yoo, Jeong-Han Yun and Taeshik Shon, Whitelist-Based Anomaly Detection for Industrial Control System Security, Journal of KICS **(2013)**, Vol.38B, No.8, pp.641-653.

[26] D. Lee, Threats according to the Type of Software Updates and White-List Construction Scheme for Advanced Security, Journal of KIICE, Jun **(2014)**, Vol.18, No.6, pp.1369-1374.

[27] Jongwook Choi, Wooram Park and Chaik Park, A Framework of Secure Access to iSCSI Network Storage based on TPM, KCC2009 **(2009)**, Vol.36, No.1D, pp.5-9.

[28] Ki-ram Lee, Nae-Hyun Cho, Hwan-woo Kwan and Chang-Ho Seo, Security and Privacy Mechanism using TCG/TPM to various WSN, Journal of KSCI **(2008)**, Vol.13, No.5, pp.195-202.

[29] Soohyun Park, Changwoo Pyo, Sunil Kim and Gyungho Lee, An Implementation of Program Counter Encoding with TPM, Journal of KIISE **(2011)**, Vol.17, No.1, pp.13-19.

Authors

박철현 (Chulhyun Park)
1999년 3월 : 육군사관학교 물리학과 졸업
2003년 2월 : 국방대학교 무기체계학 석사
2015년 2월 : 충남대학교 통계학 박사수료
2012년 10월 ~ 현재 : 육군본부 정보보호/SW정책과 사이버방호담당
관심분야 : SW 예산·기술정책, 비밀자료 정보보호론(Masking)

안훈상 (Hoon-sang An)
1987년 3월 : 육군사관학교 전자공학과 졸업
1998년 2월 : 미국 네브라스카 주립대학교 전산학 석사
2012년 9월 ~ : 아주대학교 NCW학과 박사과정
2014년 1월 ~ 현재 : 육군본부 정보보호/SW정책과장
관심분야 : 사이버전 및 대응전략, 빅데이터, 암호장비체계

김승규 (Seungkyu Kim)
1995년 2월 : 한밭대학교 전자공학과 졸업
2002년 8월 : 한양대학교 전자계산학 석사
2012년 6월 ~ 현재 : 육군본부 정보보호/SW정책과 정보보호 담당
관심분야 : 서버·네트워크 침해대응 시스템, 사이버방호체계

배종호 (Jongho Bae)
1995년 2월 : 포항공과대학교 수학과 졸업
1997년 2월 : 포항공과대학교 수학과 석사
2001년 2월 : 포항공과대학교 수학과 박사
2014년 3월 ~ 현재 : 충남대학교 정보통계학과 교수
관심분야 : 확률과정론, 대기행렬이론